LAW + INFORMATICS SYMPOSIUM ISSUE:
CYBER DEFENSE STRATEGIES AND RESPONSIBILITIES FOR INDUSTRY

ARTICLES

Threading Needles in the Dark: Will Deals Survive When Cyberattacks Collapse the Grid?
Roland L. Trope .......................................................... 339

The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law
Cassandra Kirsch .......................................................... 383

Did the National Security Agency Destroy the Prospects for Confidentiality and Privilege
When Lawyers Store Clients’ Files in the Cloud—and What, if Anything,
Can Lawyers and Law Firms Realistically Do in Response?
Sarah Jane Hughes .......................................................... 405

Commission
Susan J. Court .......................................................... 437

The Critical Role of Education in Every Cyber Defense Strategy
Juan Cayón Peña & Luis Armando García .......................................................... 459

Information Security Challenges for Companies in the Digital Age
Ors Penzes .......................................................... 471

COMMENT

Modern Developments in White-Collar Crime
R. Samuel Gilley .......................................................... 491

NOTES

The Cloud of War: Securing the Operational Domain of Cyberspace
With a Robust Military Command
Erica Hauck .......................................................... 515

Cyber Wars: Applying Conventional Laws of War to Cyber Warfare and Non-State Actors
Shaun Roberts .......................................................... 535
Northern Kentucky Law Review is published three times during the academic year by students of Salmon P. Chase College of Law, Northern Kentucky University, Highland Heights, Kentucky 41099. Telephone: 859/572-5444. Facsimile: 859/572-6159. Member, National Conference of Law Reviews. All sections which appear in this issue are indexed by the H.W. Wilson Company in its Index to Legal Periodicals. Northern Kentucky Law Review articles are also available on microfilm and microfiche through University Microfilms International, Ann Arbor, Michigan.

Subscription rates are $35.00 per volume, $10.00 per individual issue. If a subscriber wishes to discontinue a subscription at its expiration, notice to that effect should be sent to the Northern Kentucky Law Review office. Otherwise, it will be assumed that renewal of the subscription is desired.

Please send all manuscripts to the address given above. No manuscript will be returned unless return is specifically requested by the author.
SALMON P. CHASE COLLEGE OF LAW

JEFFREY STANDEN, A.B., J.D.
Dean & Professor of Law
LAWRENCE ROSENTHAL, B.A., J.D., LL.M.
Associate Dean for Academics & Professor of Law
JENNY YOUNG
Registrar of the College of Law
LISA MOORE, B.A., J.D.
Director of Career Services
JENNIFER KREDER, B.A., J.D.
Associate Dean for Faculty Development & Professor of Law

ASHELEY GRAY, B.A., J.D.
Director of Admissions
BECKY FITZSIMMONS, B.A., J.D.
Associate Dean for Administration
SHERRIE TURNER, B.S., M.P.A.
Budget Analyst
DAVID H. MACKNIGHT, B.S., J.D.
Associate Dean for Law School Advancement
MICHAEL WHITEMAN, B.A., M.S.L.S., J.D.
Associate Dean for Library Services and Information Technology & Professor of Law

FACULTY

ERIC ALDEN, B.A., M.A., J.D.
Assistant Professor of Law
DONNA S. BENNETT, A.B., M.A., M.S.L.S.
Professor of Library Services & Assistant Director for User Services
JOHN M. BICKERS, A.B., J.D., LL.M.
Assistant Professor of Law
ROGER D. BILLINGS, JR., A.B., J.D.
Professor of Law
SHARLENE BOLTZ, B.A., J.D.
Professor of Law
CAROL BREDENMEYER, A.B., M.S.L.S.
Professor of Law Library Services & Assistant Director of Faculty Services
ANTHONY E. CHAVEZ, B.S., J.D.
Assistant Professor of Law
URSULA DOYLE, B.A., M.A., J.D.
Assistant Professor of Law
NANCY L. FIRA K.B.S., J.D., LL.M.
Professor of Law
CAROL FURNISH, B.A., M.L.S.
Professor of Library Services & Assistant Director for Instruction & Outreach
JON M. GARON, B.A., J.D.
Director of Law and Informatics Institute & Professor of Law
RICHARD GRAVES, B.A., J.D., LL.M., LL.M.
Assistant Professor of Legal Writing
CHRISTOPHER GULINELLO, B.A., J.D., LL.M.
Professor of Law
AMY HALIBROOK, B.A., J.D.
Director of Children’s Law Center Clinic & Assistant Professor of Law
JACK HARRISON, B.A., J.D.
Assistant Professor of Law
THOMAS E. HEARD, B.A., M.L.S., J.D.
Associate Professor of Library Services & Associate Director for Library Services
DENNIS HONABACH, A.B., J.D.
Professor of Law
JENNIFER JOLLY-RYAN, B.A., J.D.
Professor of Legal Writing

KENNETH D. KATIK, A.B., J.D.
Professor of Law
DONALD K. KAZEE, B.A., M.A., J.D.
Associate Professor of Legal Writing
JENNIFER KINSLEY, B.A., J.D.
Assistant Professor of Law & Field Placement Program Director
MICHAEL J.Z. MANNHEIMER, B.A., J.D.
Associate Professor of Law
Jennifer Mart-Rice, B.A., M.S.L.S., J.D.
Assistant Professor of Law & Assistant Director for Collection Development, Serials and Acquisitions
BARBARA MCFARLAND
Director of Student Success Initiatives & Assistant Professor
LIJUBOMIR NACEV, B.A., J.D., LL.M.
Professor of Law
ADRIENNE NOBLE NACEV, B.A., J.D.
Visiting Assistant Professor of Legal Writing
LARRY O. PUTT, B.A., J.D., LL.M.
Visiting Professor
DAVID SINGLETON, B.A., J.D.
Assistant Professor of Law & Director of Constitutional Litigation & Indigent Defense Clinics
PHILLIP SPARKES, B.S., J.D., LL.M.
Assistant Professor of Law & Director of Chase Local Government Law Center
DONNA M. SPEARS, B.A., M.L.I.S., J.D.
Assistant Professor of Law Library Services & Assistant Director for Research and Instructional Technology
MARK M. STAVSKY, B.A., J.D., LL.M.
Professor of Law
HENRY L. STEPHENS, JR., B.A., J.D.
Professor of Law
JANE UNDERWOOD, B.A., M.L.S., J.D.
Assistant Professor of Law Library Services & Assistant Dean for Students
JOHN T. VALaurI, B.A., J.D.
Professor of Law
BARBARA WAGNER, B.A. M.S.B.A., J.D.
Director of Small Business & Nonprofit Law Clinic

CARYL A. YZENBAARD, A.B., J.D.
Professor of Law

EMERITI FACULTY
WILLIAM R. JONES, B.S., M.A., J.D.

ADJUNCT FACULTY

DONYETTA BAILEY, B.S., J.D.
DAVID BARRON, J.D.
HON. GREGORY M. BARTLETT, A.B., M.A., J.D.
JOHN BENINTENDI, J.D.
VICTORIA BOGGS, B.A., J.D.
NAIMA CLARKE, B.B.A., J.D.
ZACHARY CORBIN
ERIN CORKEN, B.F.A., J.D.
JOHN CRUZE, B.S., J.D.
PETER DEHAAN, B.S., J.D.
REBECCA DILORETO, B.A., J.D.
DAVID DORTON, J.D.
KENNETH B. GERMAIN, A.B., J.D.
ROBERT A. GOERING, JR., B.A., J.D.
ROBERT A. GOERING, SR., B.A., J.D.
WILLIAM GUSTAVSON, B.A., J.D.
MARK HARDY, J.D.
SHERYL HETTER, J.D.
PENNY HENDY, J.D.
NANCY HERBERT, J.D.
HON. STEVEN R. JAEGE, B.A., J.D.

DAVID JEFFERIES, B.A., J.D.
RICHARD KATZ, B.A., J.D.
JOHN KROPP, J.D.
JOSEPH MORDINO, J.D.
FRANK MUNGO, B.S., J.D.
DANIEL MURNER, B.A., J.D.
MARC PERA, J.D.
WILLIAM A. POSEY, J.D.
STEVEN RAY, B.A., J.D.
DEBRA ROTHSTEIN, B.A., M.A., J.D.
THOMAS ROUSE, J.D.
ANN SCHOEN, B.S. J.D.
HON. DOUGLAS STEPHENS, B.A., J.D.
HON. AMUL THAPAR, B.S., J.D.
HON. KAREN A. THOMAS, B.A., J.D.
BERNADINE C. TOPAZIO, B.A., M.B.A., J.D.
AL WESIBROD, J.D.
ELIZABETH WINCHELL, J.D.
JUSTICE DONALD C. WINTERSHEIMER, A.B., M.A., J.D.
J. STEPHEN WIRTHLIN, JR., B.A., J.D.
ELIZABETH ZINK-Pearson, J.D.
ARTICLES

Threading Needles in the Dark: Will Deals Survive When Cyberattacks Collapse the Grid?
Roland L. Trope .......................................................................................................................... 339

The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law
Cassandra Kirsch ..................................................................................................................... 383

Did the National Security Agency Destroy the Prospects for Confidentiality and Privilege
When Lawyers Store Clients’ Files in the Cloud – and What, if Anything,
Can Lawyers and Law Firms Realistically Do in Response?
Sarah Jane Hughes .................................................................................................................. 405

Susan J. Court .......................................................................................................................... 437

The Critical Role of Education in Every Cyber Defense Strategy
Juan Cayón Peña & Luis Armando García .................................................................................. 459

Information Security Challenges for Companies in the Digital Age
Ors Penzes .................................................................................................................................. 471

COMMENT

Modern Developments in White-Collar Crime
R. Samuel Gilley ...................................................................................................................... 491

NOTES

The Cloud of War: Securing the Operational Domain of Cyberspace
With a Robust Military Command
Erica Hauck .......................................................................................................................... 515

Cyber Wars: Applying Conventional Laws of War to Cyber Warfare and Non-State Actors
Shaun Roberts ......................................................................................................................... 535
Threading Needles in the Dark: Will Deals Survive When Cyberattacks Collapse the Grid?

Roland L. Trope

"The electric power industry has well-established planning and operating procedures in place to address the 'normal' emergency events . . . [But it] has much less experience with planning for and responding to high-impact events that have a low probability of occurring or have not yet occurred."


"[I]n most cases reasonable prudence is in fact common prudence, but strictly it is never its measure. . . . There are precautions so imperative that even their universal disregard will not excuse their omission."

Judge Learned Hand, The T.J. Hooper v. Northern Barge Corporation, 60 F. 2d 737, 740 (2nd Cir., 1932)

I. INTRODUCTION

This article was initially written to provide the basis for a discussion among panelists at a conference in New Delhi, in February 2014. The theme of the conference was Threading the Needle of U.S./India Deals: Safe Passage
Through Formidable Legal Risks. The theme of the panel discussion was: Threading Needles in the Dark: What Happens to Deals When Cyberattacks Disrupt the Grid for Months?

My concern in this article is not with the cyber attacks that aim at misappropriation. Such attacks have dominated headlines for several years. Their chief objective appears to have been the financial gain reaped from the exfiltration of personal identity data, business and technical data, “know-how,” source code, trade secrets, and other intellectual property. Their preferred mode of attack has usually been stealthy entry, a copious misappropriation, and stealthy departure. Damage, disruption, and destruction are usually avoided. The intruders have been thieves, not vandals. Or the intruders have engaged in espionage, but stopped short of sabotage.

Instead, I want to consider a series of kinetic cyber attacks whose aim is sabotage, designed to cripple a nation’s economy by depriving it of access to, and support of, the most critical of critical infrastructures – the reliable supply of electric power. As studies have recently observed,

A highly coordinated and structured cyber, physical, or blended attack on the bulk power system could result in long-term, difficult to repair damage to key system components in multiple simultaneous or near-simultaneous strikes. . . . [A] coordinated attack would involve an intelligent adversary with the capability to bring the system outside the protection provided by current planning and operational practices. An outage could result with the potential to affect a wide geographic area and cause large population centers to lose power for extended periods . . . Goals of these adversaries are wide-ranging and could involve extortion, societal damage, and, in the case of state-sponsored attacks, acts of war.

The interconnected grids in India and in North America are each reportedly vulnerable to long-term disruption by a kinetic cyber attack (or combined physical and cyber attacks). A coordinated, kinetic cyber attack could cause severe damage across a geographically extensive portion of the electric grid in North America. (I will refer to these incidents as “Severe Events” both in this paper and in my presentation.) The disruption would persist for months if a significant portion of the grid collapsed and if the collapse occurred, in part, as a result of damage to heavy equipment (such as transformers and generators). The greater the number of such units damaged or destroyed by the cyber attack, the longer the grid would remain down or in a state of only partial recovery.

2. The conference was jointly sponsored by the American Bar Association, Section of International Law, India Committee and by the Society of Indian Law Firms. See description at http://www.events.iceindia.in/threadingtheneedle/program.html.

The “resilience”\textsuperscript{4} of the grid is due, in part, to the performance and reliability of large power transformers (“LPTs”). As a 2012 Department of Energy (“DoE”) Report on \textit{Large Power Transformers} and the U.S. Electric Grid explained:

Power transformers are a critical component of the transmission system, because they adjust the electric voltage to a suitable level on each segment of the power transmission from generation to the end user. In other words, a power transformer steps up the voltage at generation for efficient, long-haul transmission of electricity and steps it down for distribution to the level used by customers. Power transformers are also needed at every point where there is a change in voltage in power transmission to step the voltage either up or down. Figure 1 illustrates a simplified arrangement of the U.S. electric grid system.

If such a “Severe Event” occurred, the spare units available for quick delivery and installation in-country might not be sufficient to replace those damaged.\textsuperscript{7} As a result, the required replacements might not be delivered for 8 to 14 months due to the long-lead times for procuring such units from other countries (particularly for the United States in light of the fact that such units are no longer widely manufactured in North America). In 2012 there were only six

\begin{itemize}
\item \textsuperscript{4} The term “resilience” denotes “the ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.” \textit{The National Security Strategy, The White House}, (2010), http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.
\item \textsuperscript{5} The term “LPT” as used in the DoE Report denotes a power transformer with a “maximum capacity rating of 100 MVA or higher.” \textit{Large Power Transformers and the U.S. Electric Grid, U.S. DEP’T OF ENERGY, OFFICE OF ELECTRIC DELIVERY AND ENERGY RELIABILITY}, 1 n. 2, (2012), http://energy.gov/sites/prod/files/Large%20Power%20Transformer%20Study%20-%20June%202012_0.pdf.
\item \textsuperscript{6} \textit{Id.} at 5–6.
\end{itemize}
LPT manufacturers in the United States as compared with 30 LPT manufacturers in China, and the production capacity in the U.S. is far below the U.S. market demand for such units. Although domestic U.S. production of LPTs cannot meet the current need for replacement units (and would probably be unable to cope with the need for replacement units in the event of a “Severe Event”), the situation is improving slowly with a few new LPT plants and some expansion of plants since 2012. At present, however, LPT shortage remains a serious risk if a “Severe Event” involves damage to LPTs. Any such shortage could substantially reduce the resilience of the BPS. A U.S. Department of Energy (“DoE”) report in 2012 highlighted the risk to the grid from inadequate supply of replacement LPTs: LPTs have long been a major concern for the U.S. electric power sector, because failure of a single unit can cause temporary service interruption and lead to collateral damages, and it could be difficult to quickly replace it. Key industry sources … have identified the limited availability of spare LPTs as a potential issue for critical infrastructure resilience in the United States, and both the public and private sectors have been undertaking a variety of efforts to address this concern.

LPTs are special-ordered machineries that require highly-skilled workforces and state-of-the-art facilities. Installation of LPTs entails not only significant capital expenditures but also a long lead-time due to intricate manufacturing processes, including securing raw materials.

Although reliability and redundancy are built into the system, the electricity industry identified that the limited domestic manufacturing capacity of high-voltage power transformers could present a potential supply concern in the event that many LPTs failed simultaneously.

As a result, a “New Normal” of unreliable and degraded electric power would emerge. The “New Normal” would be characterized by limited hours of electric power, rationing of such power to high priority customers, scheduled and unscheduled rolling blackouts, and unstable, widely isolated “islands” of electric power. These possibilities were anticipated and carefully analyzed in task force

---

9. As the 2012 DoE LPT Report explained, a new LPT manufacturing facility opened in Rincon, Georgia in April 2010, an LPT plant opened in Montgomery, Alabama in November 2011, a plant was expanded in Waukesha, Wisconsin in April 2012, and a new LPT production facility was scheduled to open in Memphis, Tennessee in 2013. That brings the total LPT plants in the U.S. to twelve according to a chart in the DoE Report. Id. at 26, 38.
10. For discussion of the vulnerability of the grid to a kinetic cyberattack or a combined physical and cyberattack, see pages 12 – 13 infra.
reports authorized by the North American Electric Reliability Corporation (“NERC”) and completed in May 2012. The strain on the bulk power system, as one task force report explained, concerns the fact that a “Severe Event” would take owners and operators of Bulk Power System enterprises far beyond their previous experience with extensive outages and thus “beyond the emergency response capabilities entities typically have in place”:

By definition, a Severe Event will present enormous challenges as entities within the electricity industry strive to restore and maintain reliable operations under rapidly changing circumstances never before experienced. It will not be possible to meet all electricity consumers’ demands for rapid restoration of service as entities prioritize their work with limited resources.11

A “Severe Event” would create uncertainties and confusion among commercial customers. If the “Severe Event” were caused by a coordinated cyber attack, the blackout and recovery and restoration periods would differ substantially from grid disruptions that commercial parties have previously experienced or read about. In this century, the major grid disruptions include the 2003 outage in the U.S. and Canada, the 2012 outage in India, and the storm-caused outage from Hurricane Sandy in 2012. Each covered extensive territory, affected millions of customers, caused substantial economic damage, even though the duration, compared to a “Severe Event” was days or weeks, not eight months or longer. The first of those was the widespread blackout in the Midwest and Northeast United States and Ontario, Canada, which started on August 14, 2003, and “affected an area with an estimated 50 million people and 61,800 megawatts (MW) of electric load in the states of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, New Jersey and the Canadian province of Ontario.”12 The duration of disruption seemed long at the time,


Note that a contributing factor to the long-lead procurement time of LPTs is the difficulty of transporting such heavy and at the same time fragile equipment. As the DoE Report observes:

Transporting an LPT is challenging – its large dimensions and heavy weight pose unique requirements to ensure safe and efficient transportation. . . . Although rail transport is most common, LPTs cannot be transferred over normal rail cars, because they cannot be rolled down a hill or bumped into other rail cars, which can damage the power transformer. This is because the heaviest load a railroad normally carries is about 100 tons, or 200,000 lb, whereas an LPT can weight [sic] two to three times that. A specialized railroad freight car known as the Schnabel railcar is used to transport extremely heavy loads . . . however, there are a limited number of Schnabel cars available worldwide, with only about 30 of them in North America. . . . Access to railroad is also becoming an issue in certain areas due to the closure, damage, or removal of rail lines.

U.S. DEP’T OF ENERGY, supra note 8, at 10–11.

because “power was not restored for 4 days in some parts of the United States” and parts of “Ontario suffered rolling blackouts for more than a week before full power was restored.”13 The area affected is shown in the figure below:

The disruptions in India involved the collapse on July 30, 2011 of its Northern Region Grid and, after that grid recovered, the collapse the next day, July 3114, of the Northern, North-Eastern, and Eastern Region Grids.15 Although power existed in some locations, these disruptions deprived nearly 800 million people of electricity for between one and two days.16 The areas affected are shown in the figure below:

On October 29th – 30th, 2012, Hurricane Sandy passed through New York City and “pushed inland”. In its wake, it reportedly left “more than 6 million people without power” and “impacted approximately 8.5 million customers, including businesses and services, affecting millions more people”, including the area “below 39th Street, home to more than a quarter million people . . . plunged into blackout thanks to rising waters and an explosion at a power substation on 14th Street” as well as blackouts over 17 states and caused the region to lose “between $30 billion and $50 billion in economic activity due to extensive power outages, liquid fuel shortages, and near-total shutdown of the region’s transportation system.”

The areas affected by the outages appear in the figure below:

---

17. Id.


21. HURRICANE SANDY REBUILDING TASK FORCE, supra note 19.

22. A tragic instance of a Severe Event, unrelated to a cyberattack, was what the Japanese refer to as the “triple catastrophe” of the Fukushima earthquake, the tsunamis it generated, and the flooding and breaching of the nuclear reactors at Fukushima Daiichi. Years later, the New Normal period following that catastrophe is still unfolding.
A nor’easter snowstorm that arrived a few days later exacerbated the outages and the misery and frustrations experienced by commercial and consumer customers in buildings without power, heat, or running water (the “Hurricane Sandy-Nor’Easter”).

Whatever the counterparties remember from such events would be overshadowed by one crucial fact: the owners and operators of the grid on prior occasions (as in most other blackout events) succeeded in restoring electric power to most customers within a remarkably short period (of days or a few weeks).24 As explained by the U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability in its final situation report on the Hurricane Sandy-Nor’Easter, published a month later on December 3, 2012:

All customers who are able to receive electricity and who lost power due to Sandy and the Nor’easter have had their electricity restored. The combined total peak customer electricity outages from Hurricane Sandy and the Nor’easter (reported in the DOE Situation Reports) are 8,661,527: 8,511,251 from Hurricane Sandy and 150,276 from the Nor’easter Storm, respectively. As of December 3, in New Jersey there are less than 19,000 customers and in New York there are less than 17,000 customers who are unable to accept electric service.25

24. Id.
India and U.S. counterparties to commercial transactions would expect similarly successful, relatively transparent, and reasonably prompt restoration of fully reliable supplies of electric power, even when (after some delay) they finally discover that cyber attacks caused the grid collapse. In the U.S., however, if in the midst of a business negotiation in a windowless conference room there were suddenly no light and the air conditioning ceased because of a power outage, the meeting would immediately halt, and conversation about the deal would be replaced by conversation about what happened to the electricity. If the same event occurred in India, the negotiation would continue and the conversation would remain focused on the deal, because everyone in the room (at least those from India) would expect that the backup generators that many urban office buildings have would be triggered and provide a resumption of power (restoring light and air conditioning) within 45 to 60 seconds. Such outages occur in New Delhi, for example, several times a day— and many Indian business executives and their counsel would infer (erroneously) from the way things work in India that the North American grid has a comparable resilience and that any outage would be quickly overcome by generators in the office buildings of their U.S. counterparts. In cities, such as Bangalore the regional power committee draws up a “monthly outage plan” with “outage dates approved.”

The collective interest of the panelists at the conference in New Delhi (and in this post-conference revision of this article) is in what happens to deals when that crucial expectation of rapid restoration of electricity fails to be fulfilled. The counterparties likely will shift gradually from being in denial about the severity of grid damage as the blackouts continue unabated. Their sense of uneasiness will increase when backup power supplies such as gasoline-driven generators start to fail because fuel deliveries have ceased and the storage tanks of local gas stations are empty. Cessation of telecommunications service would steadily decline and flicker out, as customers could no longer recharge phone batteries and telecom companies lacked the power to operate the cell towers.

From those and other deprivations of essential services, the counterparties will eventually appreciate that commercial activity – and urban life – had irrevocably declined. Like the grid, it would operate in “islands”, but those would be isolated and hard to sustain without frequent, unexpected disruptions. Salient features of the “New Normal” period would include:

26. For example, in January 2013, New Delhi experienced a shortage of approximately 30—400 MW of power each day, leading to “rotational load-shedding to meet the demand”. Outages were carried out deliberately also because Delhi did “not want to breach the grid code by overdrawing from the Northern Grid.” Delhi Loses Power on New Year Day, THE HINDU, NEW DELHI, (2013), http://www.thehindu.com/todays-paper/tp-national/tp-newdelhi/delhi-loses-power-on-new-year-day/article4263795.ece.

• the uncertainty of the blackouts’ duration;
• the enormity of the recovery task;
• the extent to which recovery to pre-attack levels might not be achievable in the foreseeable future;
• and, as a consequence, the unexpectedly hampered capabilities of grid operators to restore power except to isolated “islands”, stabilized through the use of “load shedding” and rolling blackouts.

Few, if any, commercial counterparties in the U.S. – and I gather in India – have contingency procedures and disaster recovery plans that address a prolonged electric power outage impeding their performance of contractual obligations or the performance of a counterparty in its own country. For the same reasons, few, if any, commercial contracts drafted in the U.S. contain provisions that contemplate or address what the parties should do in the event that a prolonged electric power outage, caused by a coordinated cyber attack, obstructs a party’s efforts to perform its contractual obligations.

Therefore, in this article, I look at the prospects for survival of India/U.S. cross-border deals in the event that a coordinated, kinetic cyber attack causes a “Severe Event” that causes damage in North America. My interest is to consider what may happen to India/U.S. commercial transactions, under their governing agreements, as the parties gradually come to the recognition that their contractual obligations need to be reviewed with counterparties, preferably in consultation with their respective counsel, in order to determine whether their deals will survive the “Severe Event” and “New Normal,” and if so, in what modified form.

A basic premise of this discussion is that relatively soon after a Severe Event, the counterparties to India/U.S. deals would need (and be well advised) to start to communicate about the predicament created by the impeded or obstructed performance of the party in the country (and region of that country) where the

28. Clients capable of contacting and conferring with counsel might receive advice to consider their options under potentially applicable provisions of their contract, its governing law, any special commercial provisions of that law, and, if not excluded by contract, any potentially applicable international conventions.

If counsel gives legal advice before the counterparties learn that the cause of the grid collapse was a coordinated cyberattack, the discovery of that unexpected cause will probably vitiate such advice, if not render it obsolete and in need of being expressly withdrawn. The value of legal advice at this point will depend significantly on a careful analysis of whether the particular event and consequences were “foreseeable” at the time that the parties entered into their contract. The answer to that question will be murky, hard to pin down, and highly dependent on facts not yet known. It may also depend on certain cautionary information or warnings that may have been transmitted to either of the counterparties by their respective government or industry regulators (e.g., such as a warning of the growing risk of cyberattacks causing damage to the grid). India and U.S. counterparties would probably be advised, among other things, to avoid taking precipitous action or communicating unreasonable, uncooperative, or provocative demands or responses, and above all, to be candid with their counterparties in any communications that broach the subject of “what shall we do” if the blackout persists for weeks or months before power is fully restored.
cyber attack collapsed the grid. That assumes, of course, that they can overcome the communications obstacles created by the blackout. Those communications, if they occur, will determine whether the parties’ deal survives (in some altered form), is terminated (without liability, or for default), or plunge the parties into an irreconcilable dispute and litigation. Exploring what shapes that outcome, and what can improve the outcome for both parties, is the focus of our discussion.

In Part II of this article, I explain how a coordinated, adaptive cyber attack on the North American bulk power system (“BPS”) might unfold through successive stages.

In Part III of this article, I consider the range of responses that owners and operators of the affected portion of the BPS are likely to attempt in order to mitigate the damage to the grid and to restore, to the extent practicable, the reliable supply of electric power to commercial customers. We will also review what will be the likely long-term effects of their inability to restore reliable supply of electric power to pre-attack levels.

Having described the progress of the cyber attack and its impact, and the limited recovery efforts that will be possible for months afterwards, I will direct attention to the India and U.S. counterparties of a commercial transaction whose performance has been halted by the partial collapse of the BPS. For purposes of discussion, I will base my observations and analysis on a fact-based scenario of an India/U.S. commercial transaction. In this transaction, the India company, “Reliable, Co.,” based in Bangalore makes navigational and environmental controls systems for use in high altitude and low orbital platforms, such as commercial aerial photography drones and telecommunications satellites.

Reliable has a long-standing relationship with an original equipment manufacturer (“OEM”) of “inertial switches” for installation on airborne platforms. “Inertial switches” detect shocks or vibrations that exceed specified limits – and then activate a safe exit system (such as an ejection seat) or deactivate or disconnect a control system (causing it to safely shut down). The OEM, “Ohmniscient, Limited,” is headquartered in Rochester, New York, and has production plants there and elsewhere in New York State. Because Ohmniscient’s products are designed to operate in demanding, low pressure, high altitude, extreme temperature environments and because it is one of the few U.S.

---

29. The Federal Energy Regulatory Commission (“FERC”) only regulates generation and transmission of electricity, not its distribution. Thus the cybersecurity standards (known as the Critical Infrastructure Protection (“CIP”) Standards) that NERC proposes and FERC approves apply only to owners and operators of generation and transmission facilities, not to owners and operators of distribution facilities. The arguably limited benefit of the CIP Standards to protect the BPS is evidenced also by the fact that “[p]ower plants under 1,500 MW are excluded even though that eliminates 70%–80% of the generation in North America.” David Savenije, Could a Cyberattack Take Out the U.S. Power Grid Today?, UTILITY DIVE, (2013), http://www.utilitydive.com/news/could-a-cyberattack-take-out-the-us-power-grid-today. “The entire distribution network is excluded, as well as small transmission assets.” Id.
makers of inertial switches for civilian and military aerospace customers, it is viewed by the U.S. Department of Homeland Security as part of the aerospace sector and thus an important company within the U.S. critical infrastructure.

Reliable and Ohmniscient have a multi-year supply agreement under which Reliable issues rolling forecasts for just-in-time delivery of inertial switches, and each forecast when it is two months out becomes a binding order under the agreement. The parties signed the agreement in December 2013.

Using that scenario, in Part IV, I explore some of the possible courses, strategies, and outcomes of the counterparties’ contractual communications as they seek to determine what they can do to help each other preserve their deal (albeit in a modified form) and to protect their respective interests while doing so.

I will conclude in Part V by considering, in retrospect, how the parties might have benefitted from including provisions in their contract that could have provided them with enhanced guidance in such a crisis. I will consider some provisional protocols for sharing information that each party might benefit from having in order to protect its interests and to understand the position and challenges being faced by its counterparty. And, I will discuss the advantages of crafting some additional flexibility into a contractual relationship in order to allow the India and U.S. counterparties to address problems that can arise from a catastrophic, widespread, and enduring loss of reliable supply of electric power that impedes or halts performance by one or both parties. That flexibility will be particularly important given the high probability that in such a crisis the parties will be at elevated risk of misperceiving and misunderstanding each other’s intentions, actions, and communications.

Throughout this article, I will examine the legal strategies that the counterparties might pursue through their communications, the challenges created by potential misperceptions and misunderstandings that could impede, distort, and frustrate their communications and legal strategies, and the risks that, despite good faith efforts by both counterparties, they might find their contractual relationship deteriorating into a costly and counterproductive dispute.

To facilitate the discussion, I have used a few conventions. First, because the author advises owners and operators of North American bulk power system (“BPS”) companies and has limited knowledge of the infrastructure and operation of the synchronous grid of India (which now includes the recently connected Southern Grid), this discussion will be limited to consideration of a partial collapse, by cyber attack, of the North American grid or BPS.

Second, because I am admitted to practice in New York and am unfamiliar with the laws and regulations of India, this discussion will use a scenario in which India and U.S. counterparties have executed a commercial contract that expressly (i) makes the laws of the State of New York the governing law of the contract, (ii) thus makes applicable to the contract the New York version of the Uniform Commercial Code (“NYUCC”), and (iii) excludes the application of the UN Convention on the International Sale of Goods.
Third, I will adopt a scenario in which the India and U.S. counterparties can be characterized as experienced in cross-border commercial deals, reasonably sophisticated in their knowledge of their contracts and in their use of legal counsel, relatively unfamiliar with the contracting practices and customs of their counterparty and its country, in the habit of diligently performing their contractual obligations in good faith, interested in developing long-term good relations with their counterparty for the financial and reputational benefits that they believe will flow from the relationship, and nonetheless quite prone to misunderstand and misinterpret the communications received from their counterparty because their respective company cultures, business customs, and commercial practices and expectations are quite different and neither appreciates just how different.

And fourth, I will use the two crucial concepts I introduced at the beginning of this article: I will refer to the causative event as a “Severe Event” and to its enduring consequences as the “New Normal”. The term “Severe Event” and its definition come from Task Force reports commissioned by the North American Electric Reliability Corporation (“NERC”) which explain that a “Severe Event”:

is an emergency situation so catastrophic that complete restoration of electric service is not possible. The BPS [bulk power system, consisting of generation, transmission, and distribution facilities] is operated at a reduced state of reliability and supply for months or possibly years through the New Normal period as illustrated below.30

II. A COORDINATED, KINETIC CYBER ATTACK TARGETS THE BPS

A. The Adversaries Pre-Positions Malware in the BPS Operational Networks

Assume that a coordinated, kinetic cyber attack has targeted a large geographic area of the Northeastern BPS. The adversaries have significant resources, sophisticated skills, and can take advantage of malware that they pre-positioned in multiple control systems within the electric power generation, transmission, and distribution stations of the BPS. An illustration of the arrangement of such stations appears in the figure below:

30. See N. AM. ELEC. RELIABILITY CORP., supra note 13, at 2.
Operating only occasionally to avoid detection, and stealthily covering their activities, the adversaries in the months preceding the launch of the kinetic attack, also injected malware into the supervisory control and data acquisition or “SCADA” systems of the BPS. They intend to activate that malware as part of an unfolding sequence of destabilizing interventions in the BPS that will cause it to damage and destroy units vital to its reliable operation. They intend to take advantage of inherent need of the BPS to remain stable, which requires a balancing of supply and demand of electricity, because:

> [E]lectric energy is generated and consumed almost instantaneously, the operation of an electric power system requires that a system operator constantly balance the generation and consumption of power.

To maintain BPS stability often necessitates rapid and correct operator detection of problems and rapid and correct input to resolve imbalances; if the proper balance is not restored quickly, the imbalances in electricity load can trigger cascading outages. As a recent MIT study explains:

> The objective of real-time operation of the electric power system is to ensure that the system remains stable and protected while meeting end user power requirements. This requires a precise balance between power generation and consumption at all times. If this balance is

32. See N. AM. ELEC. RELIABILITY CORP., supra note 3, at 3, 55.
33. Id.
maintained the system can become unstable – its voltage and frequency can exceed allowable bounds – and result in damaged equipment as well as blackouts. If the balance is not restored sufficiently quickly, a local blackout can grow into a cascading blackout similar to the ones in the U.S. in 1965 and 2003 . . .

However, when all other options for balancing power have been exhausted, the system operator must resort to proactively reducing the load, generally referred to as load shedding. . . [If load shedding fails to achieve the desired reduction in load] the system operator can initiate rotating blackouts. In rotating blackouts, groups of consumers are disconnected one at a time in a rotating fashion for a certain fixed duration (typically one hour). This disconnection is typically carried out by opening switches at the distribution substations.34

If a cyber attack can deprive operators of what is referred to as their “situational awareness” of the system, the adversaries can cause operators to make mistakes that can have potentially catastrophic effects on the stability of the grid. Such mistakes would include: failing to react (or reacting too slowly or reacting incorrectly) to load imbalances or to tripping of circuit breakers. If the attackers could disable a few substations in each of the nation’s three separate electric systems or interconnections, they could apparently cause the collapse of much of the nation’s electricity grid. A recently completed, but unpublished, study and an internal memo by the Federal Energy Regulatory Commission (“FERC”), summarized in The Wall Street Journal, details the apparent vulnerability of the grid to attack:

The U.S. could suffer a coast-to-coast blackout if saboteurs knocked out just nine of the country’s 55,000 electric-transmission substations on a scorching summer day, according to a previously unreported federal analysis.

The study by the Federal Energy Regulatory Commission concluded that coordinated attacks in each of the nation’s three separate electric systems could cause the entire power network to collapse.

A small number of the country’s substations play an outsized role in keeping power flowing across large regions. The FERC analysis indicates that knocking out nine of those key substations could plunge the country into darkness for weeks, if not months. . .

A memo prepared at FERC in late June . . . made several urgent points. ‘A Destroy nine interconnection substations and a transformer manufacturer and the entire United States grid would be down for at least 18 months, probably longer . . . That lengthy outage is possible for

several reasons, including that only a handful of U.S. factories build transformers.35

B. Alerts and Warnings Put BPS Owners and Operators “On Notice” of a Heightened Risk of Cyber Attacks Targeting the Grid – Such Attacks Are No Longer “Unforeseeable”

In my scenario, during the 21-month period preceding the cyber attack on Ohmniscient, its executive officers and Board of Directors received repeated alerts and warnings that a cyber attack appeared to be in the advance stages of planning and that apparently would target the BPS and Ohmniscient’s facilities in particular. Although the warnings and alerts initially lacked details, as threat information continued to flow into Ohmniscient it became increasingly specific,


The glue that holds the grid together is a network of transformers, the hulking gray boxes of steel and copper that weigh up to 800,000 pounds and make it possible to move power long distances. … Only a handful of companies build transformers in the U.S., and it can take weeks or months to ship transformers in from overseas. The manufacturing process itself can last more than a year, in part because a transformer can’t be bought off the shelf but rather must be made to measure for its substations. If attackers damaged enough of the nation’s 2,000 biggest transformers at critical locations, they could cause extended blackouts. Such worries moved beyond the hypothetical recently after The Wall Street Journal reported details about the attack last April on a substation that funnels electricity to Silicon Valley. Unknown gunmen shot up 17 large transformers, knocking PG&E Corp.’s Metcalf substation out of service until repairs were made.


FERC apparently did its study in response to snipers who, in a 19 minute interval, fired 120 rounds from high-power rifles, equipped with night-vision scopes, at transformers in the Metcalf Energy Center substation, located south east of San Jose, California, operated by PG&E Corp., and through which power flows into Silicon Valley. Almost every round fired struck transformers. “The transformers began to leak tens of thousands of gallons of oil. They overheated and shut down, but did not explode.” Richard A. Serrano & Evan Halper, Sophisticated but low-tec power grid attack baffles authorities, LOS ANGELES TIMES, (2014), http://www.latimes.com/nation/la-na-grid-attack-20140211,0,7627269.story#axzz2xJuUQoQ5.

The attack effectively disabled the substation, requiring intervention by operators in order to avert an outage throughout Silicon Valley. According to a Wall Street Journal account, To avoid a blackout, electric-grid officials rerouted power around the site and asked power plans in Silicon Valley to produce more electricity. But it took utility workers 27 days to make repairs and bring the substation back to life.

operation targeted, ominous, and credible. The warnings and alerts that came to Ohmniscient’s attention and were discussed in meetings of its Board included the following:

- **May 9, 2012:** NERC’s Board of Trustees approves task force reports concerning “Severe Events” that could result from a coordinated cyber attack that targets the BPS. The threat-basis scenario used in the NERC task force reports details the scenario of a successful cyber attack:

  [I]intruders take operating control of portions of the bulk power system such that generation or transmission system[s] are damaged or operated improperly.

  1. Transmission Operators report unexplained and persistent breaker operation that occurs across a wide geographic area.

  2. Communications are disrupted, disabling Transmission Operator voice and data with half their neighbors, their Reliability Coordinator, and Balancing Authority.

  3. Loss of load and generation causes widespread bulk power system instability, and system collapse within state . . . and neighboring state(s) . . . . Portions of the bulk power system remain operational.

  4. Blackouts in several regions disrupt electricity supply to several million people.36

- **February 12, 2013:** The President issues Executive Order 13636 (the “EO”) which cites “[r]epeated cyber intrusions into critical infrastructure,” characterizes their occurrence as “one of the most serious national security challenges,” and cautions that certain critical infrastructure, if affected by a “cybersecurity incident,” could result in “catastrophic regional or national effects”.

- **July 2013:** Pursuant to the EO, which authorizes DHS to share such information with critical infrastructure companies, DHS issues a formal notice to Ohmniscient informing it that if a cybersecurity incident were to involve its production facilities that it could “reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.”37 (Hereinafter referred to as a “Catastrophic Target Notice”38.)

38. For discussion of “Catastrophic Target Notices”, see Roland L. Trope & Stephen J. Humes,
November 2013: Pursuant to the EO, which authorizes DHS to share with U.S. companies nonclassified credible cyber threat intelligence about cyber attacks planned against the U.S. homeland, DHS warns Ohmniscient that it is apparently one of the known or suspected targets of attacks being planned by unidentified adversaries. (Hereinafter referred to as an “Imminent Target Notice”.)

February 12, 2014: Pursuant to the EO, the National Institute of Standards and Technology (NIST) issues the Cybersecurity Framework (“Framework”) and its “Roadmap for Improving Critical Infrastructure Cybersecurity” (“Roadmap”). The Roadmap cautions that “Poor authentication mechanisms are a commonly exploited vector of attack by adversaries” and warns of the “inadequacy of passwords for authentication. . . .”

March 2014: Articles appear in the print and online media warning of the vulnerability of the BPS to coordinated cyber attacks.

September 2014: DHS issues Ohmniscient a second, more specific and detailed Imminent Target Notice.

C. The Adversaries Set Conditions to Disguise the Source of Grid Disruptions

In our scenario, adversaries select fourth Quarter 2014 for the opportunities it presents to conceal and expand the attack. The public (and owners and operators of the BPS) have their attentions focused on the climax of the Congressional election in November. Late season tropical storms can arrive at that time (Hurricane Sandy arrived at the end of October). Early snow and ice storms can also occur. The attackers want a major event of Nature to serve as cover for their attack, making BPS operator personnel believe that they are responding to load imbalances caused by severe weather, when in fact they will be responding to a coordinated cyber attack that is adaptive, i.e., it continues and mutates for days, if not weeks, stealthily causing further disruptions, wider destruction, and thus a slower, longer recovery dominated by efforts to cope with the “New Normal”.


39. For discussion of “Imminent Target Notices”, see Trope & Humes, By Executive Order, supra note 38; and Trope & Humes, Before Rolling Blackouts Begin, supra note 38, at 715–718.


41. Id., p. 3.

42. Trope & Humes, By Executive Order, supra note 38; and Trope & Humes, Before Rolling Blackouts Begin, supra note 38, at 715–718.
The Severe Event the adversaries planned is eventually set for launch when a prodigiously large winter storm formed during an early “artic vortex” (a southward slip in the jet stream’s path that forces frigid arctic air further south than usual) was forecast to create havoc across the Northeast US and Southern Canada less than two days before the holding of the Congressional elections on Tuesday, November 4, 2014.

Seeing that forecast, the adversaries prepare to trigger their cyber attack, using malware that they had secretly injected into generation, transmission, and operating station SCADA systems months earlier. Here is how the attack unfolded from the perspective of control rooms within the BPS.

D. Essential Conditions and Key Objectives of the Cyber Attack

According to the Report of the NERC commissioned Cyber Attack Task Force:

The foundation assumption for a successful [cyber] attack that results in a blackout in several regions is that two events need to occur:

1) situational awareness needs to have been compromised and
2) there must be a bulk power system event or instability.43

1. Compromise of Situational Awareness

To compromise the situational awareness of the BPS operators (particularly those in station control rooms), the adversaries included in their injection of malware the code necessary to set up and activate a data interception and replacement device. The device will intercept data captured by the SCADA systems and replace it with “fabricated” data. This device is commonly referred to as a “man-in-the-middle” or “MITM” attack.44

The “fabricated” data, when presented to operators in control rooms, will mislead them about the actual status of their station’s portion of the BPS. Acting

43. See N. AM. ELEC. RELIABILITY CORP., supra note 13, at 12.

44. An MITM, as explained by Wikipedia “is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. . . . A man-in-the-middle attack can succeed only when the attacker can impersonate each endpoint to the satisfaction of the other – it is an attack on the mutual authentication (or lack thereof).” However, when an MITM is used to sabotage the communications between a SCADA system and control room operators, the attackers need only impersonate the data outputs to the satisfaction of the controllers. Accounts of the use of the MITM by Stuxnet suggest that Stuxnet reported data outputs on the operating conditions and rotational speed of the centrifuges (at the Iranian uranium enrichment facility at Natanz) that persuaded the control room operators that everything was functioning normally within the specified ranges, when in fact the centrifuges were repeatedly being accelerated and decelerated to speeds outside their tolerable limits. Gradually, the excessively slow and excessively fast rotational rates caused the centrifuges to self-destruct.
on such misinformation and being unaware that it is fabricated, the operators will be motivated intervene in the grid’s operation, because such information can, for example, make it appear that there is a load imbalance (insufficient supply to meet a surge in demand). The operators may well take increasingly strong actions to remedy an imbalance that has not occurred or is occurring in the opposite direction.

As a result, operation actions will further destabilize the load balance instead of restoring it. The adversaries plan to use the presentation of fabricated data on grid status repeatedly during successive phases of the attack in order to deprive BPS control room operators of an accurate grasp of situational awareness, to confuse and disorient them by having the grid appear to react contrary to operator inputs (because the inputs will be the opposite of what they should be), and ultimately to make the operators hesitant if not afraid to take any action to mitigate destabilizing occurrences within the BPS that can damage or destroy heavy generators and transformers.

2. BPS Event or Instability

To generate an instability event, the adversaries activate the payload in the pre-positioned malware inside the BPS SCADA systems. The malware “disables or impairs the integrity of multiple control systems” and enables the adversaries, working as intruders, to seize “operating control of portions of the bulk power system such that generation or transmission system are damaged or operated improperly.” At the same time, the intruders set up the MITM, confusing and disorienting control room operators, leading to the following occurrences (as depicted in NERC’s Cyber Attack Task Force Report):

1. Transmission Operators report unexplained and persistent breaker operation that occurs across a wide geographic area (i.e., within state/province and neighboring state/province).

2. Communications are disrupted, disabling Transmission Operator voice and data with half their neighbors, their Reliability Coordinator, and Balancing Authority.

3. Loss of load and generation causes widespread bulk power system instability, and system collapse within state/province and neighboring state(s)/province(s). Portions [i.e., “islands”] of the bulk power system remain operational.

4. Blackouts in several regions disrupt electricity supply to several million [perhaps tens or hundreds of millions of] people.

45. See N. AM. ELEC. RELIABILITY CORP., supra note 3, at 2.
46. Id.
BPS personnel in control rooms through that region attempt to diagnose the problem, basing much of their initial and follow-up analyses, inferences, and compensatory responses on a basic assumption: that the winter storm sweeping through the region is causing units to degrade, fail, and perhaps misreport the status of parts of the BPS.

E. Successive Phases of the Attack

During the early days of the attack, BPS operators would be misled by the MITM attack into believing that the causes of the cascading outages were related to the winter storm. They act accordingly, and unknowingly intensify the disruptions and expand the blackout area. The adversaries add to the problem by releasing additional malware in successive waves.

Because of the violent nature of the instability, and the loss of situational awareness, heavy transformers and other equipment throughout the region are damaged.

The confusion grows, particularly in the major cities throughout the region. Train service halts. Subway service halts. Traffic signals cease operating. Manhattan, for example, has no electric power, and for days the morning “rush hour” fails to occur.

The underlying cyber causes of the disruptions remain undetected for days, during which time the attack’s adaptive capabilities change the focal points of attack, the nature of the misinformation presented to control room operators, and managers of other critical infrastructure. As suspicions begin to grow that multiple, massive coordinated and adaptive cyber attacks are causing the disruptions and those disruptions begin to have national consequences (cross-sector and cross-state), the attackers challenge and take advantage of the division in responsibilities for emergency response and recovery efforts in the United States between “two distinct and different frameworks for traditional versus cyber-specific response activities.”

Guidance for responding to traditional disasters is provided by the National Response Framework (NRF), which was developed by DHS in 2008 and updated in 2010. A separate framework, developed by DHS in 2010 and known as the 2010 Interim National Cyber Incident Response Plan (NCIRP), is designed to guide response activities in the specific case of a cyber attack on critical infrastructure.

Differences and potential conflicts between the NRE and NCIRP could give rise to unnecessary debates and power struggles in the midst of a

cyber attack, when clear lines of authority and coordinating mechanisms will be most vital. These differences will also complicate efforts to build a unified system of protocols for responding to cyber events that have associated physical impacts.

[Moreover,] on issues that are vital for conducting and coordinating response operations, important distinctions exist between the NRF and NCIRP. . . . [For example,] [f]or the National Response Framework, the Stafford Act provides specific triggers for federal assistance (including the declaration of emergencies and major disasters.) The NCIRP rests on an entirely different set of thresholds provided by the National Cyber Risk Alert Level (NCRAL) system.

Most important, the two frameworks make different assumptions concerning the roles and responsibilities of state governors. Under the NRF, governors are at the heart of the process for requesting federal assistance and for engaging other response mechanisms. . . . The NCIRP specifies no remotely equivalent role for governors, even though a severe cyber attack could jeopardize the lives of citizens as much or more than any hurricane.48

In our scenario, the cyber attacks exploit these two frameworks and command structures for responses and impede decision-making, decision communication, and the vital command-and-control that was needed for clear, decisive decisions to be issued. Disagreements between agencies attempting to assist in the response and recovery delay the taking of effective measures. As a result, the attackers succeed in diversifying and expanding the disruptions and in hindering efforts to contain the growing loss of services, communication linkages, and public order.

Soon other critical infrastructure begins to degrade and break down. Gas stations quickly run out of fuel and no trucks arrive to replenish them. There is no heat or running water above the sixth floor in any of the Manhattan apartment or office buildings (and similar problems occur in Chicago, Philadelphia, and Boston). Supply-chains are strained and broken. Looting breaks out in some communities, necessitating the calling out of extra police and consideration of deploying the National Guard to restore order and assist in delivery of rationed quantities of food and water.

Food shortages appear quickly because none of the markets or restaurants are able to maintain “cold” storage for perishable foods. Federal and state governments struggle to develop and implement plans to address these problems before civil unrest erupts. Businesses attempt to resume operations with skeleton crews, but eventually accept that it is impossible.

48. Id. at 57–58.
Meanwhile, increasingly dire reports of the outage appear online and in other media in India. Counterparties throughout India view them with growing apprehension, uneasiness, and anxiety.

III. BPS OWNERS AND OPERATORS BEGIN TO REGAIN LIMITED CONTROL

During the second week of the attack and outage, the agents of the U.S. Department of Homeland Security’s Secret Service and the U.S. Justice Department’s Federal Bureau of Investigation contact owners and operators of the affected portions of the BPS and inform them that the cause of the disruption has been determined to be a coordinated cyber attack. Teams of cyber specialists are deployed to the BPS stations and begin remedial action to contain and remove the malware from the SCADA systems and other networks. By this time, however, the damage has been done and stations and begin remedial action to contain and remove the malware from the mined to be a coordinated cyber attack, the cascading outages, and the actions taken by control room operators in errant responses to the fabricated data transmitted to them by the MITM attacks.

BPS owners and operators can now focus on assessing the damage and deciding on the most urgent actions that need to be taken to start the recovery and restoration effort. They will need to identify priorities for, and key challenges to, the recovery and restoration.

As a NERC Task Force report recommends:

The first priority for system planners will be to establish communication with essential staff and recover essential planning facilities, information systems, and data needed to begin work. Once this is done, the immediate priority will be to support system operators


50. As explained at the Department of Homeland Security website, The Secret Service maintains Electronic Crimes Task Forces (ECTFs), which focus on identifying and locating international cyber criminals connected to cyber intrusions, bank fraud, data breaches, and other computer-related crimes . The Secret Service also runs the National Computer Forensic Institute, which provides law enforcement officers, prosecutors, and judges with cyber training and information to combat cyber crime. Combat Cyber Crime, DEPARTMENT OF HOMELAND SECURITY, http://www.dhs.gov/combat-cybercrime. DHS Immigration and Customs Enforcement (“ICE”) agents “conduct investigations aimed at protecting critical infrastructure industries that are vulnerable to sabotage, attack or exploitation.” Homeland Security Investigations, IMMIGRATION AND CUSTOMS ENFORCEMENT, http://www.ice.gov/about/offices/homeland-security-investigations. DHS Immigration and Customs Enforcement (“ICE”) agents “conduct investigations aimed at protecting critical infrastructure industries that are vulnerable to sabotage, attack or exploitation.” DEP’T OF HOMELAND SEC., id.
in their efforts to restore the BPS and supply electricity to customers to the extent possible on a prioritized basis. The initial surviving system will likely be in an ‘unstudied’ state. Therefore, real time assessments will need to be performed and step-by-step restoration procedures confirmed by studies before control actions are taken. ... If there is widespread damage to the system, system planning studies may need to consider using temporary configurations such as partially restored substations. Studies may include operation with less than normal margins, contingencies that may cause loss of load, reconsideration of breaker fault ratings, and reconsideration of transformer overloads.\footnote{See N. AM. ELEC. RELIABILITY CORP., supra note 7, at 48 n. 7.}

Pursuit of those priorities would have to carefully identify and address the challenges created by the Severe Event and the New Normal period. The challenges, once identified, will need to be promptly communicated somehow among the BPS owners and operators. The challenges would then also need to be communicated and clearly explained to the business communities so that each business can adjust its disaster recovery efforts in anticipation and cooperation with the plans being implemented by the BPS owners and operators.

The challenges to recovery and restoration can be appreciated if we consider those that will arise just in the efforts to stand up, maintain, and utilize “islands” of electric power after the cyber attack. The challenges related to “islanding” that have been identified by a NERC Task Force include:

- In order to operate the affected areas of the BPS “it will likely be necessary to operate in multiple electrical islands, and use emergency criteria, rotating blackouts, and a number of independent control actions to maintain the supply and demand balance and manage frequency and voltage.”\footnote{Id. at 18. (NERC explains, the use of rotating blackouts can facilitate the balancing of supply and demand for electricity by “rotating supply to different blocks of load, typically on a geographic basis, on a defined schedule or timeline.”).}

- Major electricity generation and transmission resources would probably remain unavailable for an extended period of time, and as a result, “as much as or more than 50% of total instantaneous demand cannot be served in the islands.”\footnote{Id. at 19.}

- For much of the early period of the blackout, “communication and control is impaired such that at least a portion of [electricity] switching will need manual operations by field personnel.”\footnote{Id.}

- It will become critical for BPS owners and operators to “determine the extent of the islands and which entity(s) are in ‘control’ of the surviving islands. To be in control of an island an entity needs to have the ability and decision making authority to monitor and
control the assets (generation, transmission, and load) within the island’s boundaries. This will be difficult because many of the “islands” will probably extend from one entity’s jurisdiction into another and vice versa.

• Unlike large interconnected power grids, which are “inherently stable because they have many sources of governor-controlled generation and relatively predictable load patterns,” the isolated smaller “islands” that remain or can be stood up during the weeks immediately after the attack are “high gain” systems. “[R]elatively small changes in generation or load can cause large changes in power system parameters such as voltage and frequency which may cause equipment to trip on existing protection settings.”

• “In the early stages of islanded operation, System Operators need to quickly determine their energy and capacity situation. During this time, they are likely to manage the load-generation balance using load shedding. Load shedding plans need to consider the priority or importance of loads such as critical power system loads and other dependent critical infrastructures such as telecommunications.” However, as has been learned during recent tropical and winter storms, some BPS owners and operators discover that their contingency plans have overlooked what prove to be small, but nonetheless critical infrastructure priority customers. For example, failing to include gas stations among the high priority customers can preclude the delivery of fuel needed for transportation of supplies vital for survival, such as food and water.

• “In the event of sustained rotational load shedding (rotating blackouts) communication becomes a key factor to ensure that affected areas understand what power supply they will have, at what time and for how long.”

• “Since it is impossible to predict the extent of islanding formation following a Severe Event, it may not be practical to share operational information ahead of time [whether among BPS owners or between BPS companies and other businesses]. It is important therefore that information-sharing strategies are established in preparation for such events to expedite this information dissemination and address any confidentiality concerns.” Such information sharing will need to include eventually all businesses, but initially it must include critical

55. Id. at 20.
56. Id. at 25.
58. Id. at 26.
59. Id. at 27.
infrastructure companies and a dispatch mechanism that can operate in the absence of full telecommunications service.

- Moreover, the limitations that emerge in telecommunications service will also affect the extent to which BPS owners and operators can achieve “situational awareness” over the “islands” they are trying to manage. “[A] Severe Event could create such wide spread degradation [of “island” monitoring] not to which BPS owners and operators can achieve “situational awareness” over the “islands” they are trying to manage. “[A] Severe Event could create.” Without sufficient visibility and control, system operators cannot retain reliable control of the system. “Inability to control the various parameters can lead to instability of the island and result in equipment damage.”60 In short, if “islands” are not probably controlled (which will be hard to do in these circumstances), the result will be further damage to equipment and, as a consequence, a longer period of restoration and recovery. Commercial firms will need to be prepared for a situation that does not steadily improve, but could from time to time experience sharp setbacks, equipment damage, and substantial delays to the improvement in the reliable supply of electric power.

- “Throughout the New Normal period, people will need to understand how restoration is proceeding so they can make their own decisions to care for themselves, their family, and their community. [Business owners and operators will also need to understand how restoration is proceeding.] If there is limited information available from media outlets, entities could consider posting important information (e.g., rotating blackout schedules) at government offices such as police stations and post offices and at locations where people will congregate (e.g., food and water delivery points).”61

- “Standing orders are a prescribed set of instructions for people to take action in the absence of communications or leadership direction. Standing orders could be developed to direct key personnel to report to designated locations following a Severe Event or direct a sub-station technician to clear each bus and open each breaker following a large scale blackout.”62 Standing orders will be needed by commercial businesses also as their staffs will otherwise not know whether they should act or refrain from acting, and the company officers will not know whether they are taking remedial actions, and if so, what those are likely to be.

60. Id. at 31.
61. Id. at 44.
62. Id.
Similarly, it will be important during the New Normal period to anticipate the creation of ad hoc operating relationships. Some of these relationships will need to be formed between BPS operators in stations that previously had not worked together routinely, if at all. Some of the ad hoc operating relationships will also arise between BPS owners and operators in one jurisdiction and businesses headquartered or with facilities in another jurisdiction, but now linked by an “island” that overlaps the two jurisdictions. In short, businesses may find that their electric power supplier is not their customary provider, but the BPS operator who has become responsible for maintaining an “island” that happens to include that business’ facilities. All such ad hoc operating relationships (among grid operators and between operators and customers) will be a challenge because it will involve operators communicating with and being directed by people they do not know. BPS owners and business owners and executives might find they need to establish validation protocols to confirm identities in the post-event, New Normal period, because the MITM attacks will have seriously eroded trust and made personnel wary to communicate any sensitive, useful information to unauthenticated strangers. It may even be necessary, for simplicity in opening communications channels, to “develop ‘challenge and password’ protocols or other information known only to certain persons, and to work out ways for the development, sharing, protection, and periodic changing of these passwords and other means of authenticating, without overly burdening, communications.63

Those challenges illustrate the considerable amount of orderly improvisation that BPS owners and operators will need to use during the New Normal period. As the “islands” and modes for operating them take shape, the BPS owners and operators will need to issue rules for determining priority customer access to electricity (during the periods between scheduled blackouts) and for determining who will and will not qualify as a “priority” customer at successive stages of the restoration of the BPS.

What may thus be experienced as a chaotic and rapidly changing environment by BPS owners and operators will seem much worse for any company that has not become familiar in advance with Severe Events, the New Normal that they will create, and the probable methods for coping with the New Normal that BPS owners and operators will attempt to use. That is the disaster recovery context in which the India/U.S. counterparties to commercial transactions will need to start communicating about whether their deals will survive the U.S. party’s disrupted performance, and if so, in what modified form.

In the next section, we briefly explore how some of those communications might emerge and develop. Our interest will be to examine the possible courses,

63. N. AM. ELEC. RELIABILITY CORP., supra note 7, at 42, 44, 55, 67, 78.
strategies, and outcomes of the counterparties’ contractual communications as they seek to determine what they can do to help each other preserve their deal (albeit in a modified form) and to protect their respective interests while doing so.

It is important, however, to bear in mind that we are looking at a limited set of counterparties, so they will not be seeking immediately to gain litigation advantage or to escape from deals that, before the attack, they had already determined to be disadvantageous. In other words, our discussion will exclude consideration of counterparties that seek to act in bad faith and take unfair advantage of the “opportunities” created by the Severe Event and that may enable some counterparties to gain through the catastrophe what they would not have been legally permitted to gain through performance of the contract.

IV. COMMUNICATIONS BETWEEN COUNTERPARTIES CONCERNING DISRUPTED PERFORMANCE OF THE U.S. PARTY CAUSED BY THE PARTIAL GRID COLLAPSE FROM A COORDINATED CYBER ATTACK

A. What Reliable in India May Have Learned and May Want to Know

The India buyer, Reliable, will initially learn of the blackout from a variety of sources, some reliable, some not, including news broadcasts on radio and TV, online reports, twitter feeds, etc. Misinformation will often be embedded in these reports, and will be harder to detect when it appears in traditionally reliable, vetted sources. If Reliable does not receive a direct report from its U.S. vendor,

64. Twitter has proved remarkably useful and effective during natural disasters such as Hurricane Sandy:
   As Hurricane Sandy approached the US in October last year [2012] hundreds of thousands of people used social media networks like Facebook and Twitter to keep abreast of the storm. When the dust settled, people turned to those networks again to follow recovery efforts and find out transport information . . .

   Michael Clendenin, director of media relations at Con Edison, said the @ConEdison Twitter handle that the company had only set up in June gained an extra 16,000 followers over the storm . . . .

   Aaron Donovan, media liaison at the MTA, said the agency had focused on Twitter, Flickr and YouTube in its Sandy response, but noted that ‘Twitter had the broadest pick up in a very immediate way. . . . He said that during the storm the MTA had a ‘round the clock’ social media presence. ‘First to communicate changes to service then throughout the storm itself,’ he said, but later to let people know what they are doing to update service.


65. Note that during the height of Hurricane Sandy, some news organizations such as Huffington Post and BuzzFeed suffered collapses of their servers and “turned to Twitter and other social media to deliver reports. According to Twitter, people sent more than 20 million tweets about the storm from October 27 through November 1. This was more than twice the usage from
Ohmniscient, it will have to sort through the mix of rumor and partially accurate reports in order to piece together some tactical picture of what may be happening in the blackout area and the potential impact on Ohmniscient’s operations and of its abilities to fulfill the next binding order that came into force a few days before the Severe Event.

Reliable’s executive officers view these initial events from a perspective that Indian lawyers have repeatedly told me is not uncommon for Indian business persons, particularly if they have not worked extensively in North America or Europe. They are accustomed to having to make frugal innovations, to improvise with ingenuity a quick fix or jury-rig solutions to problems that arise abruptly and are compounded by a lack of resources. The term in Hindi for the readiness and ability to make ingenious, frugal improvisations and the acceptance of the need to revert to them is “jugaad”. The term can also be less elegantly, but more practically translated as “making do with what you have”, with the implicit understanding that you are short of resources (equipment, supplies, labor, funding, etc.) and must think creatively of ways to make up the difference.

Reliable’s executives infer (quite reasonably from their perspective) from reports of a widespread electricity outage in the United States that appears to include Ohmniscient’s production facilities that the following probably describes their supplier’s circumstances at this time:

- Shortly after the outage started, Ohmniscient’s plant and offices regained full electrical power from the backup generators that it had used the two previous days. In New York, usage peaked on October 29 around 9 pm according to Twitter’s internal data, the same time that a ConEd substation exploded in Manhattan’s East Village, knocking out power to much of lower Manhattan. Emily Guskin & Paul Hitlin, “Hurricane Sandy and Twitter,” PEW RESEARCH JOURNALISM PROJECT (Nov. 6, 2012), http://www.journalism.org/2012/11/06/hurricane-sandy-and-twitter/. It is reasonable to infer that in 20 million tweets, few if any that were edited or fact-checked, that many errors in reportage occurred. Perhaps the most commonly reported error in Twitter and even in the news organization publications was that a ConEdison substation “exploded” – something the above post-Sandy quotation repeats as if it were fact. The blindingly bright multiple flashes of light that many New Yorkers (including the author) happened to see was not a substation exploding. As ConEdison’s director of media relations explained later, “the much-shared [on Twitter] ‘explosion’ that happened at the company’s 14th street power plant in Manhattan, was not actually an explosion. ‘It was more of a flash…It was a power relay that went out . . . that piece of equipment never blew up.” Id.


67. As that article explains, when a maxillofacial surgeon in India needed to reduce surgical costs for his patients, he improvised by using a steel paper clip “to keep the skin flap in place while operating”, thereby avoiding the need to use the textbook prescribed Raney clips, which are not readily available in India and are quite expensive, costing Rs 40,000 a box – or, at current exchange rates approximately $668 per box. That is a high tech example of “jugaad”. Shobita Dhar, “Surgeons do Jugaad in the Operation Theatre,” TIMES OF INDIA (Feb. 16, 2014), http://timesofindia.indiatimes.com/india/Surgeons-do-jugaad-in-the-operation-theatre/articleshow/30491175.cms.
must have as most manufacturers in India (like Reliable) similarly have;

- Ohmniscient’s supply-chain is intact, because its suppliers also have backup generators and must have had their power restored in a minute or two;

- If the outage continues for more than a day or two and Ohmniscient needs additional fuel for its generators it will readily obtain it from fuel stations that also must be running on backup generator power;

- And if Ohmniscient starts to experience any short term impediments to its continuing its production of inertial switches, its executives and personnel will “make do” – they surely practice “jugaad” in the American “can do” way.

Reliable’s executives, like many Indian executives, prefer direct communication by telephone over the use of emails and text messages. They do not think of sending an email request for an update on Ohmniscient’s situation, because it probably would not be received well, would cause unnecessary embarrassment, and is not the way Reliable’s executives would try to communicate if they thought it necessary. They would place a call, and they think there is no need to do that at this time. They do not realize that each of their inferences about Ohmniscient’s situation are incorrect, that Ohmniscient and its suppliers have been without power from the start of the outage, partly due to lack of generators and partly due to poor maintenance which rendered the available generators useless. Reliable’s executives also do not realize that a window of opportunity – partly due to poor maintenance phones of Ohmniscient’s executives – is rapidly closing, because cell phone batteries and backup batteries are almost depleted, and the continuing outages are also causing the breakdown of telecommunications in the blackout areas.

Without word from Ohmniscient (which will be difficult to obtain if the grid collapse has interrupted telecommunications services), Reliable will eventually become apprehensive about Ohmniscient’s ability to perform its contractual obligations. Those obligations will include not only delivery of the full quantity of ordered goods within the contractual schedule, but also that the delivered goods do not put Reliable at commercial risks by failing to meet contractual requirements. Reliable will want to watch out for failings that occur when a manufacturing firm experiences stresses that can be imposed by a blackout and the resulting compromise of its production methods and supply chain. Such failings could include:

- *Goods that are substandard or otherwise nonconforming*, which may occur if Ohmniscient’s high quality production methods have been compromised or degraded by –
equipment damage (from electrical spikes),
irregular operation (from rotating outages),
insufficient manpower (from the inability of staff to get to the production plant),
equipment malfunctions (from inexperienced replacement staff operating the equipment improperly or adjusting the controls incorrectly), or
inadequate quality control (from management decisions to give priority to continuing some level of output, rather than maintaining product quality;

- **Goods that are counterfeit or contain counterfeit parts**, which may occur if the blackouts have impeded performance by Ohmniscient’s suppliers, and they have resorted to buying counterfeit parts in order to ensure they make timely deliveries to Ohmniscient; and

- **Goods that contain hidden defects**, which may occur if the cyber attacks included releases of malware through offshore updates to firmware included in Ohmniscient’s products.

As reports indicate that the blackouts will continue for weeks, if not longer, Reliable may confer with its legal counsel to discuss what communications it should start to have with its troubled and silent U.S. vendor.

At this stage, Reliable probably limits its legal consultation to its lawyers in Bangalore. However, Indian counsel may recommend that U.S. counsel be engaged to help advise on the contract, because it is expressly governed by New York law and it would be prudent to interpret it in light of decisions by the courts of New York, both state and federal.68

Reliable asks its Indian counsel what assurances it should seek concerning Ohmniscient’s ability to fully perform the supply agreement, what questions it should consider asking in order to understand Ohmniscient’s situation and recovery efforts, and what assistance or relief from obligations it might consider offering in order to help the contract survive the stresses and impediments created by the cyber attack and collapse of the BPS. They map out the points to

---

68. Foreign governments, overseas companies, and multi-national corporations headquartered in foreign jurisdictions routinely engage U.S. legal counsel to advise and represent them on issues relating to application of U.S. law or on negotiations with U.S.-based entities. Usually such representations remain confidential. However, a top-secret document obtained by former N.S.A. contractor Edward J. Snowden revealed that one U.S. law firm, Mayer Brown, had its communications monitored by the N.S.A.’s Australian counterpart, the Australian Signals Directorate, while the law firm was representing the Government of Indonesia in trade talks with the United States. James Risen & Laura Poitras, Spying by N.S.A. Ally Entangled U.S. Law Firm, THE NEW YORK TIMES (Feb. 15, 2014), http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html?_r=0.
be put in a draft letter, and discuss how to get it delivered. Indian counsel recommends that the letter be transmitted by email or fax to a colleague at a U.S. law firm located outside of the blackout area with a request for her to find a way to get it delivered to Ohmniscient’s offices in Rochester, New York and to obtain a reply, if possible via the same messenger or delivery service.

B. What Ohmniscient in New York May Have Learned of the Blackout Area

Meanwhile, Ohmniscient may want to address and reduce concerns it anticipates that Reliable might be having regarding the ability of its U.S. supplier to perform and deliver on schedule. In addition, Ohmniscient may want to start to put itself in a position to be relieved of liability for any damage to Reliable that may flow from the interruption of Ohmniscient’s production lines and the consequential delay of its performance of its contract to supply initial switches to Reliable. Before attempting to communicate with Reliable, Ohmniscient manages to contact and confer with its local New York counsel.

Ohmniscient discusses with counsel the possibility of declaring an event of excusable delay (i.e., an event of *force majeure*), and whether the Severe Event and its surrounding circumstances would qualify as an event of excusable delay under the *force majeure* clause in the supply agreement and in light of whether a Severe Event caused by a cyber attack was a foreseeable occurrence at the time the parties entered into the agreement (in December 2013). They discuss an alternative strategy: declaring that continued performance of the contract is “impossible” and should be terminated without fault or liability by either party. And, they discuss possibly communicating with Reliable to see if it might be receptive to discussions that would extend the time and conditions of Ohmniscient’s obligations to perform in exchange for a reduction in the unit price of the inertial switches, and thereby enable the contract to survive, in amended form, and to spare the parties a potential dispute over Ohmniscient’s entitlement to an event of excusable delay.

C. Correspondence Exchanged on “Impossibility” of Performance and of Ohmniscient’s Entitlement to Declare an Event of Excusable Delay

Reliable and Ohmniscient exchange written correspondence. Reliable asks for an assessment of the situation and in particular of the extent to which the blackout has obstructed, or is likely to impede, Ohmniscient’s ability to perform its short and long term contractual obligations and Ohmniscient’s current plans to overcome such obstacles, resume production and delivery of product. Reliable offers to start discussions of ways in which it can help Ohmniscient overcome the obstacles created by the loss of electrical power, ranging from a relaxation of the delivery schedule and quantity per delivery to using its good relationships with component suppliers in Asia to provide Ohmniscient with parts that its suppliers are finding that they cannot deliver during the early stages of the New Normal period.
Reliable’s correspondence reflects its senior officers’ experience with city-wide, and sometimes state-wide, shortages of electricity. Not infrequently (outside of Mumbai), the local power corporation may impose simultaneous scheduled outages across sectors of a city, for a period of days.\textsuperscript{69} At other times, unscheduled outages occur, causing production lines to halt until diesel powered backup sources of electricity are brought online by a manufacturer or until the power company can restore electricity.\textsuperscript{70} Indian companies are also well aware of how much worse the electricity shortages are in Pakistan, severely curtailing

\textsuperscript{69} An IEEE Spectrum article in 2007 reported that: Planned load shedding is common, especially in rural areas, although cities, including the megacities of Delhi and Kolkata, are not immune: utilities cut power to customers for hours at a time to balance load and generation capacities and in so doing keep the generators turning between 48.5 and 50 hertz, the frequency specification of the Indian electric system. …Blackouts occur when load so far outstrips generation, either because of the loss of a generator or a major transmission line, that the frequency dips to 47.5 Hz. At that point, the generators automatically trip off and a blackout ensues. For example, on 25 February India’s western grid went down, and the citizens of Maharashtra were without power for several hours. But as always, Mumbai was mostly spared. Both Tata and Reliance invoked ‘islanding’ schemes, whereby they take the city off the national grid and supply customers with power from their own local plants until the larger network comes back up. First deployed by Tata in the late 1960s, the separation happens only when the integrity of the system cannot be maintained despite automatic emergency load shedding.


Moreover, the North American grid operates on tight frequency control (with grid frequency remaining in a niche of +/- 0.03 Hz of the rated frequency and any excursion beyond that triggers alarms) and all control areas adhere to their respective interchange schedules. In India, the situation is quite different and causes frequent daily outages:

- Industries and commercial establishments need back-up diesel generators for continued operation when power supply from the grid is cut-off or is curtailed (for a few hours every day), and domestic consumers have to bank on their own battery-backed ‘inverters’ to get the basic amenities of light and fan round the clock. … Frequency is the most crucial parameter in the operation of an A.C. system. The rated frequency in India is 50.0 Hz. While the frequency should ideally be close to the rated frequency all the time, it has been a serious problem in India. … Frequency fluctuations are caused by load-generation imbalances in the system, and keep happening because consumer load keeps changing.


\textsuperscript{70} See N. AM. ELEC. RELIABILITY CORP., supra note 7, at 42, 44, 55, 67, 78.
production across entire industries,\footnote{As explained in a November 2013 article: Today, crippled by the shortages of electricity that have paralyzed this country in the past five years, most of the machinery [in textile maker Chenab Ltd.] stands idle. . . . For households, life can seem preindustrial. Refrigerators don’t run, children can’t do homework in the dark. . . . ‘The people of Pakistan have practically given up on assuming they will have power.’ . . . The goal [of Pakistan’s government] is to bring the outages down to eight hours a day and eliminate them altogether in five years . . . . Saeed Shah, *Power Outages Hobble Pakistan’s Biggest Exporters*, THE WALL STREET JOURNAL (Nov. 29, 2013) http://online.wsj.com/news/articles/SB10001424052702304795804579097620?KEYWORDS=pakistan+power+outages &mg=reno64-wsj.} and even prompting the Pakistan Government to enter into negotiations for a linking of the electric grids of the two countries in order for India to sell Pakistan electricity than it cannot otherwise obtain.\footnote{Progress of the negotiations between the two countries can be inferred from reports by The Wall Street Journal in July 2013 and The Telegraph Tribune and The Express Tribune in March 2014, respectively: India has warmed up to arch-rival Pakistan by offering to help its neighbor resolve an acute power shortage that has plunged its cities in hours of darkness and blighted economic growth, two senior government officials confirmed Friday. New Delhi is in discussion for building a trans-border power grid over the next three years to export electricity...India is considering a grid corridor that can carry 500 megawatts to 1,000 MW electricity, easing Pakistan’s electricity deficit of 25%, power ministry officials say. Saurabh Chaturvedi, *India, Pakistan Discuss Joint Power Grid*, THE WALL ST. J. (July 5, 2013) http://online.wsj.com/news/articles/SB100014241278873248586721967356036?KEYWORDS=pakistan+india+electricity+deal&mg=reno64-wsj. A team of Indian technicians is reviewing the draft agreement on the export of 500 mega watts (MW) of power to Pakistan. . . . Officials indicated that if all technical aspects were resolved, electricity trade between the two countries could start before the end of this calendar year. . . . Officials said there was a broad agreement that cross-border trading would be through high voltage direct current (HVDC) coupling as is being done with Bangladesh at present. This will ensure that both the grids operate independently. . . . The World Bank, which had done the pre-feasibility study for the energy trade between the nations, has suggested the two countries should consider scaling up the trade to 1,200MW to meet the long-term energy demand of the Islamic nation. . . . Pakistan faces a 37 per cent, or 5,000 MW, energy shortage. . . . At present, Islamabad imports 35MW of power from Iran. It plans to increase this to 100MW. It is also considering importing another 1,000MW from Tajikistan. R. Suryamurthy, *Push for Pak Power Trade Pact*, THE TELEGRAPH (Mar. 30, 2014), http://www.telegraphindia.com/1140330/jsp/business/story_18134355.jsp#.UzdRQ7-f9ic. See also Zafar Bhutta, *Pakistan all set to Import Electricity from India*, THE EXPRESS TRIBUNE (Mar. 20, 2014), http://tribune.com.pk/story/685056/pakistan-all-set-to-import-electricity-from-india/.} 

In its reply, Ohmniscient provides a deeply pessimistic assessment, and mentions its diligent efforts to overcome the obstacles created by the loss of electrical power, acknowledges but postpones consideration of Reliable’s offers of relief or assistance, and emphasizes that it might soon find it is excused from further performance for the following reasons: performance has been rendered “impossible” or, as New York courts tend to refer to it “commercially
impracticable”,73 or circumstances have arisen that entitle Ohmniscient to declare an event of excusable delay. Ohmniscient’s letter relies on a brief explanation it has received from its legal counsel concerning each of those grounds of excused performance.

New York law recognizes two bases for contractual impracticability. First, under Section 261 of the Restatement Second, Contracts, a party’s obligation to render performance is discharged if it has been made “impracticable without his fault by the occurrence of an event the nonoccurrence of which was a basic assumption on which the contract was made at”74. Second, under Section 2-615 of New York’s version of the Uniform Commercial Code (“NYUCC”), a nonperforming or breaching seller is excused from continuing performance of the entire contract under the following conditions75:

(a) Delay in delivery or non-delivery in whole or in part by a seller who complies with paragraphs (b) and (c) is not a breach of his duty under a contract for sale if performance as agreed has been made impracticable by the occurrence of a contingency the non-occurrence of which was a basic assumption on which the contract was made or by compliance in good faith with any applicable foreign or domestic governmental regulation or order whether or not it later proves to be invalid. [(b) is not applicable to Ohmniscient] [(c) The seller must notify the buyer seasonably that there will be delay or non-delivery. . . .76

Crucial to a party seeking to qualify for either ground of excused performance is that the cause(s) that make continued performance impossible must at the time of the signing of the contract have been unforeseeable.77 The contract between Ohmniscient and Reliable must also not contain any expression of an intent that seller Ohmniscient, the nonperforming party, assumed the risk of such event or contingency or that the parties otherwise agreed to allocate that risk to Ohmniscient. The Ohmniscient/Reliable contract contained no such language. Therefore, Ohmniscient’s challenge to establish excused performance will center on whether the cause of commercial impracticability was not foreseeable at the time the parties entered into the contract. Ohmniscient’s executives would like to interpret foreseeability as exceedingly narrow, because the more narrow and

---

75. This brief summary of NYUCC §2-615 omits certain caveats contained in therein, including exceptions made for substitute performance and situations that affect only a part of the seller’s capacity to perform. Here the assumption is that Ohmnisicent is facing the prospect of being unable to continue or resume performance of any of its production and delivery obligations to its customer Reliable.
specific the foreseeability requirement, the more it appears to them that neither party did foresee (or even could have foreseen) the string of causes that has made Ohmniscient unable to continue performance. From Ohmniscient’s perspective, the parties did not foresee that a kinetic cyber attack would target the grid, would be successful, and would so damage equipment that a “Severe Event” (to use NERC’s term) occurred, *i.e.*, that for an extended period of weeks or months electricity service cannot be restored to pre-attack levels and without such power Ohmniscient cannot continue to manufacture or deliver the inertial switches to Reliable.

New York courts, however, do not construe the “foreseeability” requirement under UCC §2-615 to require that hindsight be the measure of foreseeability, or that the foreseeable be measured by what the parties could only have known after the fact by reading media accounts. Instead, as one New York court explained it:

> [The] foreseeability requirement does not entail contemplation of a specific contingency; rather, it is sufficient that the contingency that eventually occurred could have been foreseen as a real possibility that would affect performance. [citation omitted] Although it does not appear that [they] ever contemplated a train derailment . . . common sense dictates that they could easily have foreseen such an occurrence.78

Furthermore, New York courts tend to limit impracticable or impossible performance to situations in which the means of performance have been destroyed by an act of God or of nature (i.e., a natural cause that could not have been prevented by the exercise of prudence, diligence, and care). New York courts also tend to construe the doctrine narrowly. Thus, if financial difficulty or economic hardship is the cause, “even to the extent of insolvency or bankruptcy,” the courts will usually not excuse performance.79

---

78. Id.

Aware of that rather broad and highly discretionary construction that New York courts tend to put on “foreseeability”, counsel for Omhnsicient drafts a letter that emphasizes that neither party foresaw nor could have foreseen that what appears to possibly have been a combination of weather and cyber attacks and maybe even negligence by Omhnsicient’s electricity supplier could have led to a widespread outage that has already lasted longer than anyone initially thought it would and now appears to be likely to continue indefinitely because the affected BPS enterprises are now refraining from declaring when full service will be restored or even if it can be in the foreseeable future. The letter, however, makes somewhat heavy-handed use of the applicable legal terms and even mentions some applicable case law and cites the NYUCC.

Omnisci’s letter reflects arguably too much of a self-serving tone and detail, and perhaps not enough of a candid disclosure of the facts to really protect Omhnsicient’s interests. The letter makes no mention of any of the alerts or warnings that came to the attention of Omhnsicient’s executive officers and Board of Directors, including the pre-contract receipt from DHS of a Catastrophic Target Notice and of an Imminent Target Notice. It is also important to recall that New York common law implies in every contract a duty to perform it in good faith. Therefore, the letter writing strategy employed by Omhnsicient counsel has taken a serious risk of appearing to fall short of that good faith standard. The letter contends that the parties could not have foreseen the events of the cyber attacks and collapse of the grid. However, the DHS notices and wide-spread reports warning of such events and such outcomes, and the fact they appeared before the parties entered into the contract, made such events arguably foreseeable to Omhnsicient. By taking such positions without disclosing what Omhnsicient’s Board actually knew could be viewed by a court later as a lack of candor and as seeking an excuse of performance on knowingly dubious, if not unjustifiable, grounds.

Omnisci’s reply is thus rather legalistic and maneuvering, especially to Indian business executives and is thus viewed by Reliable and its Indian counsel as disappointing, uncooperative, and somewhat confrontational. The letter, moreover appears surprisingly counter-productive when it is Omhnsicient whose performance has halted and Reliable whose interests, with its customers, is thus being put at increasing risk with each passing day of delay.

Reliable’s Indian counsel recommends, and Reliable agrees to engage, a New York law firm to serve as co-counsel to help avert an impasse, ensure Reliable knows its options under the applicable law, and to help interpret and negotiate any invocation of the force majeure clause. That clause, in the supply agreement, reads as follows (with text in bold indicating portions marked with a yellow highlighter by Reliable’s New York counsel):

Event of Excusable Delay. A Party hereto shall not be in default on account of, or be liable or responsible for, its nonperformance or the consequences arising from its nonperformance under this Contract if caused by an occurrence that is not reasonably foreseeable or otherwise
caused by or within the reasonable control of the nonperforming Party and without its fault or negligence ("Event of Excusable Delay"). Such occurrences include, without limitation, acts of God or the public enemy, acts of a government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather (e.g., hurricanes, tornadoes), earthquakes, widespread power outages, and delays of common carriers despite such Party’s reasonable efforts to prevent, avoid, delay, or mitigate the effect of such acts, events or occurrences, and which events or the effects thereof are not attributable to a Party’s failure to perform its obligations under this Agreement.

Over the course of the next few weeks, Reliable and Omnisicient intensify their negotiations of what they can and will do to and those negotiations determine whether their contract will survive, and if so, with what modifications. The salient positions taken and revised by the counterparties in their correspondence (written increasingly by their respective counsel) can be summarized as follows:

- Omnisicient advanced reasons supporting its entitlement to declare an Event of Force Majeure, noting that no country has previously suffered a geographically extensive and prolonged blackout caused by a cyber attack, that the intensity and damaging nature of the attack was “unforeseeable,” that the event and its consequences were beyond the “reasonable control”, and that despite the company’s diligent efforts, it was unable to mitigate or overcome the consequences of what was being referred to by NERC and the U.S. media as a “Severe Event”. Omnisicient, however, recognizes that the contract’s Force Majeure clause presents several obstacles that it might not be able to overcome, including that it details the performance excusing events but omits mention of cyber attacks and grid collapse and it emphasizes that any performance excusing event must “not be reasonably foreseeable” whereas Omnisicient received credible cyber intelligence from the DHS that warned of and put it on notice of imminent cyber attacks and there were published responsible reports of the increased risk of such attacks on the grid with outages being a possible result.80

80. Some courts note the list of events in a contract clause, and if they do not include the event at issue, will hold that force majeure does not apply, because “ordinarily, only if the force majeure clause specifically includes the event that actually prevents a party’s performance will that party be excused.” Kel Kim, 519 N.E.2d at 296; see Bende & Sons, 548 F. Supp. at 1022. However, if a contract clause is phrased in more general terms, does not attempt a list of specific events, and the parties did not have knowledge of such events or negotiate their possible occurrence, then New York courts may find the nonperforming party excused by the force majeure. See, e.g., One World Trade Ctr. LLC v. Cantor Fitzgerald Secs., 789 N.Y.S.2d 652 (N.Y. Sup. Ct. 2004) (where the lease at issue detailed a few events, but expressly expanded the scope of force majeure by adding “it being agreed that the foregoing enumeration shall not limit or be characteristic of such conditions
• Reliable responded politely and firmly that it was its understanding that the test for “impossibility” of performance was a very stringent test that emphasized that there had to be such a material change in circumstances and so impossible to perform the work that the contract had been deprived of its material purpose.  

Reliable reasoned that it was premature to make determinations of impossibility or force majeure, and would remain so until the parties had explored in depth Reliable’s offers of assistance and to relax contractual obligations.

• In a subsequent exchange of correspondence, Ohmniscient describes in detail the challenges created by the New Normal, its location outside the boundaries of even the nearest “island” of electricity, and continues to insist on its entitlement in light of these developments to declare an event of force majeure but it refrains from making such declaration.

• In response, Reliable asks some pointed questions about circumstances that prevailed when the parties were negotiating the supply agreement. For example, did Ohmniscient receive a formal notice from the U.S. Department of Homeland Security (“DHS”), issued pursuant to Executive Order 13636, informing the company that if it were to be damaged by a cyber attack, the consequences locally or nationally could be “catastrophic”? Did Ohmniscient receive a formal notice from DHS warning it that based on U.S. intelligence sources, a cyber attack had been planned against the U.S. homeland and Ohmniscient was believed to be one of the main targets? In other words, was Ohmniscient one of the over 3,000 companies that reportedly received such notices in 2013? 

Between February 2013 (when Executive Order 13636 was issued) and December 2013 when the parties signed the supply agreement, had Ohmniscient made any preparations to defend against and recover from a severe cyber attack? Did it make or enhance such preparations between the

or circumstances” which are “beyond the control of the Port Authority or which could not be prevented or remedied by reasonable effort and at reasonable expense. . . . The defendants are sophisticated commercial tenants and there is no reason to excuse them from the operation of the force majeure clause which they freely negotiated.); see also Burke v. Steinmann, No. 03 CIV. 1390, 2004 WL 1117891, at *9 (S.D.N.Y. May 18, 2004) (the court rejected a defense of force majeure was based on the aircraft flown into the World Trade Center towers and where the dispute concerned a brewery not located at or in the neighborhood of the World Trade Center “even though those terrible events caused financial hardship for many businesses in New York.”).


83. See Kerner, supra note 49.

time that it received such notices from DHS and when the parties signed the supply agreement? Did its electricity supplier receive similar notices? Were there not reports in the U.S. media that several major BPS enterprises had received such notices?

- In a brief reply, Ohmniscient acknowledged that it had, indeed, received an Imminent Target Notice in September 2013 warning it that it was a target of a cyber attack that could occur at some indeterminate time, for an indeterminate duration, and of an indeterminate severity. It expressly declined to confirm or disconfirm whether it had received in June 2013 a Catastrophic Target Notice (cautioning that damage to it from a cyber attack could reasonably result in catastrophic harm locally or regionally). It eventually believed the Imminent Target Notice to be a “false alarm,” and similarly regarded a later notice of the same vague content received in September 2014, just two months before the Severe Event that damaged and widely disrupted the BPS. As for the other kind of notice (that damage to it would result or cascade in damage regionally or nationally), Ohmniscient did not comment, and when asked again in a subsequent correspondence from Reliable, Ohmniscient pointed out that such notices were described in Executive Order 13636 as “confidential”⁸⁵ and it therefore could neither confirm nor deny having received one.

- As the trend in this correspondence reveals, the parties gradually moved first towards a legal impasse and disagreement, then drew back from it as Reliable’s questions and Ohmniscient’s answers gradually made evident that a cyber attack of the severity experienced and that damaged the BPS so extensively was not so clearly “unforeseeable” at the time the parties entered into the contract, that it had been described in NERC reports, and that the information sharing authorized by Executive Order 13636 and implemented by DHS in its notices to Ohmniscient put that company on notice that it was at elevated risk of being targeted by a cyber attack and it also knew that its electricity supplier (among others) had been similarly put on notice of a severe cyber attack.

- In short, Ohmniscient began to have doubts that it could declare an Event of Force Majeure and have a court sustain its entitlement to do so under the language of the supply contract. Moreover, Reliable had pointed out that the express list of events of force majeure did not include mention of a cyber attack or other cyber event, and reasoned that a New York court might well view that as a decision by the parties to exclude such event or at least evidence

---

⁸⁵. *Id.*
that they had not thought it important enough to include it as a basis for an excusable delay or relief from liability.86

- What finally capped the withdrawal from the legal impasse (or pre-litigation precipice) appeared to be Reliable’s inclusion in a correspondence of an invocation of Article 2-609 of the NYUCC (Right to Adequate Assurance of Performance),87 a recitation of the challenges that Ohmniscient had referenced in its several post-event correspondences, and a formal request that Ohmniscient give Reliable “adequate assurances” that it would successfully complete performance of the contract notwithstanding the challenges it had described previously in such detail. Ohmniscient’s counsel warned the company that it needed to coax Reliable into a negotiation, because a failure to give such assurances might entitle Reliable (under Article 2-609 of the NYUCC) to deem its supplier, Ohmniscient, to be in anticipatory breach88 of the contract.

As we learned during the panel discussion at the Delhi Conference,89 the nature of the arrangements that Reliable and Ohmniscient eventually agreed upon and reflected considerable adjustment to the cultural differences between the parties assumptions of the resilience of the BPS, the limited abilities of U.S. parties to gain access to generator supplied power during grid outages, and their quite different expectations and approaches to commercial exigencies during a national crisis involving collapse of the grid. The adjustments would be reflected eventually in a formal amendment to the supply contract, and in some improvised changes in their customary course of dealing. They adopted this course of action from having learned lessons from watching other India/U.S. counterparties reach mutually beneficial resolutions and from reading about a few horrible instances in which the India/U.S. counterparties sued each other and began a long, costly, and ultimately wasteful series of legal battles before panels of international arbitrators and judges of courts in their respective countries.

V. RECOMMENDATIONS

Until a "Severe Event" of the kind described in the Reliable/Ohmniscient scenario has actually been experienced, it is premature to express a definitive set of “lessons learned” or to offer precise recommendations for how India/U.S. counterparties, like Reliable and Ohmniscient, might facilitate their resolution of future crisis when those result from a Severe Event of cyber attacks that extensively damage the electric grid in either country. I will therefore only offer

86. See Kelley, supra note 73.
88. Id.
89. The panelists were: Laurel Bellows (The Bellows Law Group, P.C., Chicago), Sajai Singh (J. Sagar, Associates, Bangalore), Pavan Duggal (Pavan Duggal Associates, New Delhi), Sanjeev Mehra (Tata Power Trading Co. Ltd., Uttar Pradesh, India), and the author Ronald L. Trope.
only a few recommendations here. I would emphasize that these recommendations should be viewed as provisional, and subject to what may be learned during an actual "Severe Event" and, in anticipation of such Event, from officers and directors in consultation with counsel giving serious consideration to how a "Severe Event" might affect commercial parties at different stages of the crisis:

- *Force majeure* clauses should not be assumed to be a “one-size-fits-all” remedy for catastrophic events, even those that are of the high impact, low frequency variety;

- If a *force majeure* clause gives a list of illustrative unforeseeable events, then parties would do well to review their boilerplate *force majeure* clauses to see if they need to be updated to identify any major type of risk that has been increasingly receiving significant attention by heads of state, legislatures, industry regulators, the media, and others who shape the public awareness of risks and the courts’ view of what has now become “foreseeable”;

- Re-evaluations of *force majeure* clauses and deliberations of advice to give clients seeking to position themselves to be relieved of contractual obligations of performance (without incurring liability) should be informed also by an awareness of formal information sharing by governments with their country’s critical infrastructure companies, since such notices may well alter the calculus for determining whether certain catastrophic or highly disruptive events were “foreseeable”, or were actually somewhat within the control of a party (to avert or mitigate) to an extent not previously appreciated until one considers what the party should have done once it was “put on notice” by its government of an elevated risk of a cyber attack.

- Counterparties located in different countries with substantially different cultures and business practices should consider holding informal discussions about whether they want their contracts to survive certain worst case scenarios, like the Severe Event and New Normal period following a damaging cyber attack on a nation’s electric grid. The more interested they find that they are in giving their contract enhanced chances of survival of such circumstances, the more effort they should consider investing in drafting and negotiating some of the following contractual provisions:
  - ✓ Mechanisms for sharing information during disruptive events and the New Normal periods that may follow;
  - ✓ Procedures and pre-positioned resources for creating communications channels in the event that normal telecommunications become attenuated, unreliable, or unavailable for sustained periods;
Protocols for exploring ways for a performing party to assist a non-performing party when conditions resembling an event of force majeure arise and the parties might benefit from contractually expressed guidance in the event that normal telecomm definitive agreement gives the parties considerable flexibility to work through their initial loss of communications, early misgivings, premature or overly aggressive demands for assurances, and tendencies to maneuver for position instead of managing the crisis for the mutual benefit of the parties.

Whatever additional recommendations might be worth adding should be left to the imaginations and judgment of counsel to companies in India and the United States as they contemplate the growing risks to cross-border transactions from cyber attacks that could bring down large sections of the grid in the United States or in India. However, as such incidents and consequences become increasingly foreseeable and cross-border trade increases between the two countries, counterparties should consider reviewing with counsel the boilerplate provisions of their standard commercial and corporate contracts to see if the now foreseeable cyber incidents make it compelling to revise customary provisions such as force majeure and indemnification. It might also be worth considering having counsel draft new provisions to address communications, cyber threat information sharing, and response and recovery plans that will be stress-tested in the event of a successful kinetic cyber attack on a nation’s interconnected grid.

To overcome cultural differences and potential misunderstandings at the start of such emergencies and throughout the “New Normal” of a crisis lasting several months or longer, the parties will need flexibility in their contracts. They will also find particularly helpful something more than the usual boilerplate provisions because a collapse of the grid and degradation of electricity supplies for months will bring all parties beyond their experience with weather-caused disruptions and the usual recovery from such incidents. The parties will therefore need some provisional road maps that let each know how the other will try to respond so that if they are unable to communicate they might nonetheless have some reasonable basis for inferring what each other will attempt to do in good faith to ensure the survival of their deal and the benefits each sought to obtain when they entered into it. The investment in developing such “road maps” is not substantial. Counsel and client need to think carefully and it may be that consideration in detail of a scenario between parties like Omniscient and Reliable will help in clarifying the challenges and on that basis in drafting provisions to help parties cooperate and be prepared for their respective efforts at “jugaad” or “making do” with the scarcities imposed on them by the loss or rationing of electricity from a cyber attack that targets the grid and causes a “Severe Event”, months long disruption never before experienced by companies in the United States or India.
THE GREY HAT HACKER: RECONCILING CYBERSPACE REALITY AND THE LAW

Cassandra Kirsch*

“Borders and boundaries pose no obstacles for hackers. But they continue to pose obstacles for global law enforcement, with conflicting laws, different priorities, and diverse criminal justice systems. With each passing day, the need for a collective approach—for true collaboration and timely information sharing—becomes more pressing.”

Robert Mueller
Director of the Federal Bureau of Investigation (2012)

I. INTRODUCTION

From the Sony Media “data breach war” with LulzSec to the hacktivist breaches of the Arab Spring, media and security experts have coined 2011 as “The Year of the Hack.”1 During the year, hacking and data breaches flooded the headlines—at least “58 highly-publicized hacking attacks occurred in 2011 with victim organizations around the world ranging from law enforcement agencies, Fortune 500 companies, and governments to defense agencies and military contractors.”2 Prior to 2011, few people knew about the Guy Fawkes mask wearing hacker group “Anonymous”3 or even fathomed hackers being able to topple entire corporate and government computer networks. Despite much of the media attributing the incidents to “Anonymous,” the Year 2011 revealed vast

* J.D., University of Denver Sturm College of Law (2013); B.A., The University of Texas (2008). The author would like to extend special thanks to Professor John T. Soma, the Executive Director of the University of Denver Privacy Foundation, for his encouragement, mentorship, and support of her research on the cross-section of needs between privacy, high technology, and security.


2. Clayton, supra note 1.

diversity and motivations among numerous hacking subgroups, including LulzSec and AntiSec.4

In light of these breaches and a burgeoning cyber crime industry, the Federal Bureau of Investigation (“FBI”) has invested considerable resources over the last few years into the FBI’s Cyber Division in an attempt to address today’s increasingly sophisticated and evolving cyber threats.5 Once a tertiary priority for the FBI, cyber crime stands to overtake terrorism in rank.6 Nonetheless, rather than subside, hacking incidents continue to increase in number and scope.7 The 2013 Target breach affected nearly a third of the U.S. population,8 and the FBI

4. See Chloe Albanesil, Did Anonymous Hack Sony’s PlayStation Network or Not?, PC MAG. (May 4, 2011, 5:15 PM), http://www.pcmag.com/article2/0,2817,2384919,00.asp; Agence France-Presse, Hacker group AntiSec declares ‘war’ on U.S police, THE RAW STORY (Aug. 6, 2011, 6:15 PM), http://www.rawstory.com/rs/2011/08/06/hacker-group-antisc-declares-war-on-u-s-police/; Hao Li, Sony hacked again, LulzSec claims, INT’L BUS. TIMES (Jun. 2, 2011, 4:26 PM), http://www.ibtimes.com/sony-hacked-again-lulzsec-claims-287969; Kevin McCaney, AntiSec hackers expose data from 74 sheriff’s offices, GCN (Aug. 8, 2011), http://gcn.com/articles/2011/08/08/antisc-hack-74-sheriffs-data.aspx; Jason Schreier, Sony Hack Probe Uncovers ‘Anonymous’ Calling Card, WIRED (May 4, 2011, 2:08 PM), http://www.wired.com/gamelife/2011/05/sony-playstation-network-anonymous/. During 2011, media organizations were quick to label any hack as an attack by Anonymous. For example, the now infamous hack of the PlayStation Network was first attributed to Anonymous, but was really organized by LulzSec. Compare Schreier, supra note 4, with Albanesil, supra note 4, and Li, supra note 4. AntiSec, similarly, has been called a “wing” of Anonymous, although it has taken on its own hierarchy and separate hacking exploits. See McCaney, supra note 4; Ryan Gallagher, Anonymous splinter group AntiSec wages war on ‘profiteering gluttons,’ THE GUARDIAN (Feb. 27, 2012, 6:00 PM), http://www.theguardian.com/technology/2012/feb/27/anonymous-splinter-group-antisec-waging-war.


6. See FBI Director: Cybercrime will eclipse terrorism, CNN MONEY (Mar. 2, 2012, 7:55 AM), http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/index.htm (statement of FBI Director Robert Mueller) (“Terrorism does remain the FBI’s top priority, but in the not too-distant-future we anticipate that the cyberthreat will pose the greatest threat to our country.”).


warns that attacks similar to the Target breach “will continue to grow in the near term” despite its efforts.\footnote{Anjli Raval, \textit{FBI warns retailer of more cyber attacks}, \textit{FIN. TIMES} (Jan. 24, 2014, 12:14 AM), http://www.ft.com/intl/cms/s/0/e52517f8-8480-11e3-b72e-00144feab7de.html#axzz2xrKor42x. The Recent Cyber Intrusion Events Directed Toward Retail Firms report confirms that 20 hacking cases in 2013 involved the same kind of malicious software used against Target Corp; Jim Finkle & Mark Hosenball, \textit{Exclusive: FBI warns retailers to expect more credit card breaches}, \textit{REUTERS} (Jan. 24, 2014, 12:53 AM), http://uk.reuters.com/article/2014/01/24/us-target-databreach-fbi-idUKBREA0M1UF20140124. The report provides details the risks posed by “memory-parsing” malware that infects point-of-sale (POS) systems, which include cash registers and credit-card swiping machines found in store checkout aisles.}

FBI officials admit the agency is losing the “War on Hackers:”\footnote{Devlin Barrett, \textit{U.S. Outgunned in Hacker War}, \textit{WALL ST. J.} (Mar. 28, 2012, 10:31 AM), http://online.wsj.com/article/SB100014240527023047710457730773326180032.html.} it is no longer a question of who will be hacked, but when.\footnote{Robert S. Mueller, III, Dir., Fed. Bureau of Investigation, \textit{Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies}, Address at the 2012 RSA Cyber Security Conference (Mar. 1 2012), available at http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.} Due to the low entry costs into the cyber crime market,\footnote{See Anthony Wing Kosner, \textit{Target Breach Of 70 Million Customers’ Data Used Bargain Basement Malware}, \textit{FORBES} (Jan. 15, 2014, 11:44 PM), http://www.forbes.com/sites/anthonykosner/2014/01/15/blackpos-malware-used-in-target-attack-on-70-million-customers-retails-for-1800/ (noting that the malware used in the Target breach, BlackPOS, is available on underground cyber crime forums for as low as $1,800).} number of computers involved in transnational commerce, and shortage of available law enforcement,\footnote{Mueller, supra note 11.} cyber crime has become a growth industry.\footnote{See Tony Bradley, \textit{Cybercrime: A Recession-Proof Growth Industry}, \textit{PC WORLD} (Feb. 5, 2011, 8:44 PM), http://www.pcworld.com/article/218850/cybercrime_a_recession_proof_growth_industry.html.} Effectively combating cyber crime requires existing laws and the roles of federal and local officials to evolve. In building the nation’s collective capabilities to fight the cyber threat, we “need to look at alternative architectures that are more secure . . . that allow critical infrastructure owners and operators to better spot threat actors and to provide information to law enforcement to track and to catch them.”\footnote{Mueller, supra note 11.} Given the complexities of investigating and regulating cyber crime, law enforcement and the legislature should take note from some progressive corporate vendors and consider an unlikely ally in the hacker community: the grey hat hacker.

To the general public, “hacker” is a term synonymous with a member of the cyber criminal underground, but not all hacking is created equal. Indeed, the purpose, techniques, and intent of hackers differ greatly within the international hacking community. From political hacktivists, to the hacker posting software.
security flaws on a public forum, to the Paypal hackers selling personal information on the black market, people hack for a number of reasons. Within these various subgroups of hacking, hackers largely fall into three “shades” of hats recognized by the security industry: white hat, black hat, and grey hat.\textsuperscript{16} White hats are members of the security industry hired specifically to find security flaws, whereas black hats break into systems for no other reason than to commit a crime of some sort or to profit.\textsuperscript{17} Somewhere in between the two extremes is the grey hat hacker, operating on the fringe of civil and criminal liability to report security vulnerabilities.\textsuperscript{18}

Although largely absent from the 21st century mainstream hacker narrative, grey hat hacking has been around since at least the mid-1990s.\textsuperscript{19} Collectively, “grey hats” form a sort of neighborhood watch in cyberspace, contributing an essential element of self-governance and consumer protection.\textsuperscript{20} Enlisting the assistance of technologically-savvy individuals who are disproportionately exposed to risk may influence the safety of the Internet in ways that other legal solutions, primarily criminalizing certain behavior, cannot.\textsuperscript{21} Corporate vendors, such as Google and PayPal, have already begun tapping into this security resource through incentivizing reports of security flaws through their bug bounty programs.\textsuperscript{22} However, this sub-group of the hacking community operates, regardless of participation in bug bounty programs, under exceedingly low thresholds for both criminal and civil liability.\textsuperscript{23}

The intersection between grey hat hacking activities and legal realities resurfaced in 2012 with the controversial and heavily publicized verdict of \textit{United States v. Auernheimer}.\textsuperscript{24} Andrew “Weev” Auernheimer and Daniel Spitler, members to the “grey hat” group Goatse Security, published on the Gawker website a vulnerability affecting over 100,000 iPad customers on

\begin{itemize}
\item \textsuperscript{17} Id.
\item \textsuperscript{18} Id.
\item \textsuperscript{20} See Hoffman, supra note 16.
\item \textsuperscript{22} Enid Burns, \textit{Microsoft Woos Hackers with Bounties for Bugs}, E-COMMERCE TIMES (June 21, 2013, 9:55 AM), http://www.ecommercetimes.com/story/78331.html.
\item \textsuperscript{23} See Hinkley, supra note 21.
\end{itemize}
AT&T’s website.\textsuperscript{25} The vulnerability would leak e-mail addresses to anyone who typed a ICC-ID into the URL bar (search bar).\textsuperscript{26} In other words, any customer could access his or her account data by going to an AT&T URL containing their iPad’s unique numerical identifier: no password, cookie, or login procedure was required to bring up a user’s private information. Nonetheless, the two were charged under the Computer Fraud and Abuse Act (“CFAA”) for “unauthorized access” and the verdict was returned against them.\textsuperscript{27} The verdict has been heavily criticized by security professionals: the verdict of \textit{Auernheimer} disincentivizes cyber security researchers from finding security flaws, which in turn makes the rest of us less safe on the Internet and frustrates the efforts of corporate bug bounty programs.\textsuperscript{28}

This paper focuses not only on the current state of the law regarding grey hacking, but also what a legal regime that recognizes grey hacking as a legitimate part of the security industry could and should be. Part I examines the history and motivations within the grey hat hacking community. Part II discusses the legal implications of recent interpretations of the CFAA on the grey hacking community, and Part III looks at recent corporate endeavors to incorporate grey hacks into their security regime and whether doing so provides a feasible alternative to the status quo. Part IV looks ahead and proposes a Congressional response to resolve the inconsistencies between cyber space realities and jurisprudence by updating the language of the CFAA and creating a safe harbor provision for the grey hat community. Through establishing proper incentives and safe harbors for the grey hat hacker, private and public entities can take better advantage of the wealth of untapped talent and initiative behind much of the technological progress on the Internet.

\begin{footnotesize}
\textsuperscript{25} Id. After discovering the flaw, the two wrote a script – which they dubbed the “iPad 3G Account Slurper” — to mimic the behavior of numerous iPads contacting the web site in order to harvest the e-mail addresses of iPad users. According to authorities, they obtained the ICC-ID and e-mail address for about 120,000 iPad users. \textit{Id}.

\textsuperscript{26} See \textit{id}.


\textsuperscript{28} See Anna-Maria Taliharm, \textit{INTERNATIONAL CRIMINAL COOPERATION IN THE CONTEXT OF CYBER INCIDENTS 55} (2011) available at http://books.google.com/books?id=PeKssuU7kDoC&dq=investigating+cybercrime+jurisdiction+challenges&lr=&source=gbs_bookshelves_s. One of the major challenges of cybercrime investigations is that even when investigators manage to locate the criminals, taking them into custody may not be possible due to lack of jurisdiction over them. Jurisdiction is one of the major constraints that affects the results of cybercrime prosecution. \textit{See generally} Marc D. Goodman & Susan W. Brenner, \textit{The Emerging Consensus on Criminal Conduct in Cyberspace}, 2002 U.C.L.A. J.L. & TECH. 3, (2002), available at http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php. Indeed, extradition treaties require “double criminality” in order to extradite an individual, i.e., they require that conduct be a crime in the jurisdiction where it was committed, as well as in the jurisdiction seeking to extradite an offender. \textit{Id.}, at 1.
\end{footnotesize}
II. THE ADVENT OF A HACKING MIDDLE GROUND—THE GREY HAT

Grey hat hacking describes hacking exploits to discover security weaknesses in a computer system or product with the goal of bringing the security weaknesses to the attention of the owners (albeit often by public notice on a forum). Essentially, the end goal of a grey hat’s activities is the same as the white hat hacker: exposing vulnerabilities in public and government systems to improve system and network security, while promoting advances in technology and consumer protection. Although this sub-group of the hacking community usually does not hack for personal gain or malicious intent, a grey hat often is prepared to break the law through exploiting security, network vulnerabilities without prior consent or authorization in order to achieve better security.

The term “grey hat” first entered the mainstream in 1999 when the New York Times ran an exposé on the hacker collective, L0pht. L0pht adopted the term “grey hat” to represent those in the hacking community who neither adhere to the malicious activities of the “black hats,” nor share the same sentiments of the law-abiding, often corporate employed, “white hats.” Instead, the grey hats encompass independent computer researchers that publish online advisories upon discovering security flaws in commercial-network software. These advisories, however, create a catch-22 by simultaneously providing both a detailed description of the flaw with enough information for others (without respect to their hacker classification) to duplicate the “exploit” and a solution that tells network administrators how to close the loophole. Nonetheless, grey hat hackers would rather take the risk and notify the public first. The L0phites described this aversion to first notifying the vendor in terms of consumer protection: their tips were often “swept under the rug” and the users of the computer network would never know the risk to their data. Such disillusionment is still prevalent a decade later among many grey hats.

31. Id.
33. Id.
34. Id.
35. Id. (“If a black hat approaches us and says, ‘Hey, this is the project or problem I’m looking at . . . ’ we’ll talk to them, no problem. And if a government agency approaches us and says, ‘How do you do this,’ or, ‘How does this work,’ we’ll talk to them.”).
36. Id.
Unfortunately, the claims of the grey hats are grounded in reality. Despite pervasive and accelerating cyber-threats, the FBI reports that private organizations in general either “don’t recognize [the reality of cyber-threats], they don’t understand [or] they don’t care.” Moreover, the existing legal regime helps perpetuate this status quo of inaction. Forty-six states have enacted commercial data breach notification laws, but the breach of a network alone is often not enough to require notice to consumers. Rather, the duty to notify consumers generally comes into effect only after the business develops a reasonable belief or determines that the personally identifiable information has actually been “accessed” or “acquired.” In other words, the vendor is free to “decide not to release a patch because a cost/benefit analysis conducted by an in-house MBA determines that it’s cheaper to simply do . . . nothing.” Even if the vendor decides to patch the security flaw after notice, patches are sometimes left undeployed anywhere from a few months to more than a year later. Over the last decade, Microsoft, in particular, has come under fire for repeatedly neglecting to deploy patches. In 2001, Microsoft kept secret for nearly two months the UPnP vulnerability in Windows XP and more recently in 2013 failed to deploy a patch for over two months after notice that a bug in Skype allowed attackers to hijack another user’s Skype account. Each vulnerability required only a minute


41. Id. (“Vendors are typically held accountable to shareholders, who have a primary goal of profit. This means that if there’s no money to be made doing an activity, such as generating patches; most organizations will do whatever is likely to have the least possible cost.”).


43. See Mathew Schwartz, Skype Deals With Account Hijacking Exploit, INFO. WK. (Nov. 14, 2012, 11:26 AM), http://www.infonewsweek.com/security/vulnerabilities/skype-deals-with-account-hijacking-explo/240134937. “Before Skype made that fix, using the vulnerability to hack into a Skype account was ‘child’s play,’ according to Rik Ferguson, director of security research and communication at Trend Micro . . . . ‘All that was necessary was to create a new Skype ID, and associate it with the email address of your victim. Once this procedure was complete, a flaw in the password reset procedure allowed the attacker to assume control over the victim account by using the online password reset form. This would lock the victim out of their Skype account and allow the hacker to receive and respond to all messages destined for that victim until further notice.’” Id.
level of time and skill to repair.\textsuperscript{44} Nevertheless, Microsoft is not alone in these criticisms: the hacking and security communities have scrutinized the respective failures of Apple\textsuperscript{45} and PayPal\textsuperscript{46} to repair vulnerabilities for months at time following notice.\textsuperscript{47} Given the track record of vendors across industries, grey hats turn to what they perceive as the only ethical place that will use a zero-day discovery:\textsuperscript{48} the consumer.\textsuperscript{49}

Although grey hats expose security flaws in the name of the public good and Internet safety, law enforcement and white hats condemn grey hats for harboring ulterior motives, specifically the self-serving humiliation of corporate entities. Arguably, such drive for humiliation comes in large part from both the aforementioned vendor negligence and lack of liability for such negligence. The recent verdict in \textit{Auernheimer} highlights this continued criticism of grey hat ulterior motives, and the drive for such originating in vendor negligence. Prosecutors in \textit{Auernheimer} alleged in their complaint that the Defendants went out of their way to exact the greatest reputational damage to AT&T,\textsuperscript{50} pointing to 150 pages in the complaint of chat logs where Spitler and Auernheimer admitted conducting the breach, in part, to tarnish AT&T’s reputation.\textsuperscript{51} Without a doubt, Defendant Auernheimer’s behavior was self-serving, but a closer analysis of the complaint reveals a far more altruistic motivation for his behavior in an earlier e-mail to the U.S. attorney’s office in New Jersey. In his letter, Defendant


\textsuperscript{47} See id.

\textsuperscript{48} “Zero-day” refers to a previously unknown vulnerability in a computer application. Because developers have had zero days to address and patch the vulnerability, an exploitation of the vulnerability occurs on “day zero” of awareness of the vulnerability. \textit{What is a Zero-Day Vulnerability?}, \textit{PC Tools}, http://www.ptools.com/security-news/zero-day-vulnerability/ (last visited Jan. 15, 2014).

\textsuperscript{49} See \textit{Auernheimer}, supra note 40.


Auernheimer complained that “AT&T needs to be held accountable for their insecure infrastructure as a public utility,” further elaborating that “we must defend the rights of consumers, over the rights of shareholders” because it is the public “who would have been harmed had AT&T been allowed to silently bury their negligent endangerment of United States infrastructure.”

Ulterior motives or not, the harm of disclosure to the un-patched masses greatly outweighs any benefit that comes from shaming vendors when the public has little to no recourse for security breaches. The majority of courts have dismissed data breach claims brought by affected persons that did not suffer any appreciable injury: simply having one’s personal information lost or stolen may not be sufficient to establish standing to claim damages. Even in cases where the evidence indicates negligence by a corporation caused a data security breach and resulting harms, causation and damages are often difficult (if not impossible) to prove. A recent case in point is the dismissal of the class action brought against Sony Media for the various security breaches and flaws brought to light by the two-year LulzSec War. With “170,000 employees and over $88 billion in revenue over . . . 12 months,” Sony customers expected the corporation would respond with security safeguards when “a PS3 user successfully ‘jailbroke’ his PS3 console and posted instructions for doing it.” When Sony did not respond, even after widespread media coverage of the breaches, Sony customers brought a federal class action lawsuit. Despite the widespread nature of the breach and evidence of Sony’s failure to enact appropriate security safeguards, the Judge ultimately decided to dismiss the lawsuit for being void of damages as “none of the named plaintiffs subscribed to premium PSN services, and thus received the PSN services free of cost.” Additionally, while Sony customers accused the company of misrepresenting the quality of its protections,

52. Criminal Complaint, supra note 50, at 6.
57. Id. (stating that US District Judge Anthony Battaglia dismissed charges including negligence, restitution and unjust enrichment).
all PSN users signed a Sony Privacy Policy that included “clear admonitory language that Sony’s security was not ‘perfect,’” and therefore “no reasonable consumer could have been deceived.”59

Electronically stored data might literally be priceless. In most security breaches, there is no way to accurately estimate how many computer users have not only discovered a flaw, but also exploited it. As a result, tracing the effects and identifying the scope of the harm is near impossible. With the difficulty in obtaining recourse for consumers, near inherent vulnerabilities found in networks, and near absence of liability for vendors, grey hat hackers (regardless of any personal, secondary motives to humiliate a corporate entity) can fill the void left by this lack of assurances for consumer data protection on vendor websites. However, the current legal environment affords grey hat hackers no protection as all hacking is essentially illegal under the dominate federal statutory framework: the Computer Fraud and Abuse Act (“CFAA”).

III. LEGAL IMPLICATIONS OF THE CFAA AND THE GREY HAT HACKING COMMUNITY

The CFAA was enacted in 1986 as a response to growing political and media attention surrounding the dangers of computer crime.60 Three years prior to the CFAA, 1983’s War Games introduced much of the country to the “hacker” and sensationalized the dangers of hacking in a heated Cold War environment.61 The influence of War Games was not lost on members of Congress, describing it as “a realistic representation of the automatic dialing and access capabilities of the personal computer.”62 With these Hollywood representations in mind, the CFAA criminalized exceeding authorized access to a protected computer system, making it a felony when trespass leads to damages over a certain monetary threshold.63 From 1986 to 1996, the CFAA underwent major revisions and was further strengthened by the USA Patriot Act of 2001. While the revisions broadened the CFAA to account for ever-evolving cyber crime threats, the CFAA has become so broad that the law now “threatens to swallow the Internet.”64

Under the CFAA, overly expansive or uncertain interpretations of “unauthorized access” do not provide sufficient notice of prohibited activities for both computer users and law enforcement alike. Exactly what constitutes an

59. Id. at 968.
61. WarGames (United Artists 1983).
"access," and what makes an "access" unauthorized, is presently unclear. The language "intentionally access a computer without authorization or exceed authorized access" could very well turn ordinary people into criminals for things many do routinely, such as scan an online matchmaking site at work or lie about personal information on Facebook. Alternatively, the language may prohibit accessing a computer in a way that either violates a contract or widely shared norms of computer use. Indeed, in the 2010 iPad hack, the Defendants did not anticipate that the CFAA would be invoked against them for accessing information by typing information into a search bar.

The broad language of the CFAA is a result of out-dated Internet philosophies from before the Internet's omnipresence in society. Congress rooted the statute in common-law trespass doctrines, specifically the concept of restricted authorization. Under the concept of restricted authorization, a person commits trespass not only when he or she enters property or a portion of it when told not to, but also when a person enters for some purpose other than what they are authorized. However, common law property doctrine is difficult to apply in situations such as the recent Auernheimer case. While the Court in Auernheimer ruled Auernheimer's activities constituted the type of "hacking" outlawed by the CFAA, many security experts dispute whether hacking actually took place when Auernheimer and Spitler accessed an unprotected computer available to the public on the World Wide Web. According to the facts of the case, AT&T did not require any special credentials to get to the unencrypted customer information. No username or password was needed to access the user information, as any computer user could change a string of numbers in the URL

65. See Orin S. Kerr, Cybercrime’s Scope: Interpreting “Access” and “Authorization” in Computer Misuse Statutes, 78 N.Y.U. L. REV. 1596, 1630 (2003) (“Although courts have struggled to distinguish between these two phrases, prohibitions against exceeding authorization appear to reflect concerns that users with some rights to access a computer network could otherwise use those limited rights as an absolute defense to further computer misuse.”).


67. Criminal Complaint, supra note 50, at 10. Defendant Auernheimer believed that while there “absolutely may be legal risk,” it was “mostly civil.”


69. See Williams v. Garnett, 608 S.W.2d 794, 797 (Tex. Civ. App. 1980) (“Under the doctrine of trespass ab initio, recognized in Texas, a person who enters upon real property lawfully pursuant to a conditional or restricted consent and remains after his right to possession terminates and demand is made for his removal becomes a trespasser from the beginning, and the law will then operate retrospectively to defeat all acts done by him under color of lawful authority.”).


bar accessible on any computer with Internet access. Rather, AT&T made the private information of its customers publicly available, without any encryption or other security measure, failing to provide any notice or indication that it was not deliberately publishing its customer database or required authorized access to view.

Moreover, white hat security professionals criticize the Third Circuit ruling in Auernheimer for failing to take into account the realities of security research, setting a dangerous precedent that could restrict the abilities of grey and white hats alike. If the CFAA equates unrestricted web page access with unauthorized access under the CFAA, the line between malicious hacking and researching for security vulnerabilities (or merely visiting a website at all) becomes increasingly blurred. The vagueness of CFAA, and the verdict of Auernheimer that follows from the broad language of the CFAA, gives cyber security researchers a disincentive to find security flaws, which makes the rest of us less safe on the Internet.

IV. PRIVATE SECTOR INCORPORATION AND RECOGNITION OF THE GREY HAT HACKING COMMUNITY

When technology companies and vendors must prepare for the inevitable hack, the disincentive to report security flaws created by current interpretations of the CFAA does not bode well for the fight against cyber crime or protection of consumer data. Although there is no such thing as perfect security, encouraging the reporting of security flaws is necessary when two internal factors plaguing vendors are unlikely to disappear anytime soon: industry standardization and human error.

73. ICC-IDs in an URL bar are not passwords, but rather serial numbers associated with iPads. They are more adequately equated with a username, which focuses on an account associated with a person (not the means to access the account). The numbers in the URL bar are just numbers that enable each account page to appear at a specific Internet address.
75. Id. (“Researchers will be more circumspect about what they are willing to disclose. They’ll fear that they might be the next Weev.”); see also Andrew Couts, Why conviction of the AT&T iPad ‘hacker’ is a problem for us all, DIGITAL TRENDS (Nov. 21, 2012), http://www.digitaltrends.com/mobile/att-ipad-hacker-auernheimer/; Robert Graham, You are committing a crime right now, ERRATA SECURITY (Nov. 20, 2012), http://erratasec.blogspot.com/2012/11/you-are-committing-crime-right-now.html; and Ben Weitznenkorn, Security Experts Blast iPad Hacker’s ‘Chilling’ Conviction, TECHNEWSDAILY, (Nov. 26, 2012, 1:09 PM), http://www.livescience.com/25020-ipad-hacker-guilty-security-research.html. (“Security experts tend to agree with Auernheimer’s attorney, Tor Ekeland, who told Ansel Halliburton that the verdict should concern ‘any legitimate security researcher,’ because Auernheimer and Spitler didn’t hack through any security on the AT&T website.”).
Contrary to the portrayal by the media, hacking is not an elite field limited to a small society of cyber geniuses. Many of the more infamous corporate data breaches were conducted using SQL injection, a very common (albeit devastating) tool of the hacker trade. In fact, SQL injection is generally recognized as one of the top cyber attack techniques on the Internet. SQL code, an international programming language designed for managing data in relational database management systems (“RDBMS”), serves as the current industry-standard for website database language. SQL injections alter the predefined logical expressions within a predefined query by injecting operations which always result in true or false statements, in turn, allowing hackers to run random SQL queries and extract sensitive user information from applications or bypass security mechanisms and compromise the backend of server or network. Consequently, SQL injection is a natural weapon of choice for hackers around the world. The standardization of websites makes hacking multiple databases that much easier—the Achilles’ heel of one website is often the same as another.

Even in a perfect world where cyber security experts could produce an impenetrable website, human error would still undermine these efforts. Often considered the weakest link in cyber security, human error is a specific variety of human performance that is so clearly and significantly substandard and flawed when viewed in retrospect that there is no doubt that it should have been viewed


77. Id. (“We see SQL injection as the top attack technique on the Web,’ said Michael Petitti, chief marketing officer at Trustwave, a security firm whose clients include Heartland.”). See also Noa Bar-Yosef, The Most Prevalent Attack Techniques Used By Today’s Hackers, SECURITY WEEK (Sep. 23, 2011), http://www.securityweek.com/most-prevalent-attack-techniques-used-todays-hackers.

78. See, e.g., KEVIN KLINE ET AL., TRANSACT-SQL PROGRAMMING 52 (1999); Orest Halustchak, Proposed Spatial Data Handling Extensions to SQL, in TOWARDS SQL DATABASE LANGUAGE EXTENSIONS: FOR GEOGRAPHIC INFORMATION SYSTEMS 69 (VINCENT B. ROBINSON & HENRY TOM eds.,1993); DEJAN SARKA, ITZIK BEN-GAN, LUBOR KOLLAR & STEVE KASS, INSIDE MICROSOFT® SQL SERVER® 2008: T-SQL QUERYING 273 (2009).


80. Aaron B. Brown, Oops! Coping with Human Error in IT Systems, ACM QUEUE (Dec. 6, 2004), http://queue.acm.org/detail.cfm?id=1036497. (“[P]sychology tells us that mental-model mismatches, and thus human error, are inevitable in the rapidly changing environments characteristic of IT systems.”) See also Human Error Causes Most Data Loss, Study Says, PC WORLD (Mar. 12, 2007), available at http://www.pcmag.com/article/129736/article.html. A report from the IT Policy Compliance Group reveals that user error is responsible for half of all sensitive data losses, with policy violations -- either deliberate or accidental- accounting for another 25 percent.

by the practitioner as substandard at the time the act was committed or omitted.\textsuperscript{82} People, with their unique capacity for (often unintentional) ingenuity, even manage to break systems designed for dependability and integrity. In 2011, the hacking of HBGary Federal during the Super Bowl was made possible through both an amateur SQL injection to break into one of HBGary’s servers from the back-end database coupled with human error.\textsuperscript{83} While the SQL injection alone was not enough to access the main HBGary site, luck would have it for the hackers that HBGary’s CEO, Aaron Barr, used the same password (kibafo33) for all of his accounts.\textsuperscript{84} One of the first steps and basic tenets of cyber security is not only to have a secure password, but also not to have the same password for multiple accounts (especially classified and unclassified).\textsuperscript{85} Here, an experienced cyber security official failed to follow one of the most basic and widely-known tenets of cyber security law. If an experienced cyber security official could fall victim to human error, then the same error could feasibly happen with another human-monitored computer network.

As much as “we want to stay away from the adversary, as much as we want to stay away from the bad things that people do, the only way we can understand what’s going on is to interact to some degree with that community.”\textsuperscript{86} Cyber crime is prolific, in part, because it is difficult to police; perpetrators enjoy a certain level of anonymity\textsuperscript{87} and deterrence though fines or jail time are diluted for a number of reasons.\textsuperscript{88} The threat environment has become so complex and ubiquitous that the most promising security requires utilizing members of the hacking community that understand how the more malicious hackers intend to exploit security flaws and will “penetrate the security of [websites] in order to show that the security is insufficient and that [the companies] should increase it.”\textsuperscript{89}

\begin{thebibliography}{9}
\bibitem{84} Parmy Olson, \textit{Anonymous Strikes Back}, SALON (June 3, 2012, 1:00 PM), http://www.salon.com/2012/06/03/anonymous_strikes_back/.
\bibitem{87} See Jay P. Kesan and Carol M. Hayes, \textit{Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace}, 25 HAR. J.L. & TECH. 415, 418-419 (Spring 2012) (“It is almost impossible to accurately and consistently identify attackers, which severely complicates any steps that might be taken to uncover those responsible and hold them accountable for their actions.”).
\bibitem{88} See \textit{id.} (stating that “law enforcement and judicial action against malicious cyber intrusions currently do not present enough of a practical threat to deter potential attackers”).
\bibitem{89} Hartley, \textit{supra} note 86.
\end{thebibliography}
Along those lines, the corporate sector has attempted to recruit the skills of independent security researchers, specifically grey hat hackers, through “bug bounty programs.” A handful of companies, such as Google, PayPal, and Facebook, now offer rewards (sometimes in the six-digit range) for hackers who shore up company software, thus “keep[ing] hackers and malware out.” Bug bounties serve as a way for companies to make products more secure while engaging with hackers, many of whom would be looking for the vulnerabilities anyway. Though bug bounty programs are becoming increasingly more common, no widespread consensus exists among corporations as to the benefits or feasibility of these programs. Some companies like Adobe believe that bug bounties should only be used to catch malevolent hackers due to the risk of “double-dipping” by hackers. Nonetheless, even without an industry-wide consensus, this increasing trend shows a growing level of acceptance and perceived licitness of some areas of hacking.

What’s most troubling for the grey hat hacking community about these bug bounty programs is that nearly all hacking under bug bounty programs remains illegal if the contractual language of the program is not properly crafted. For example, Google’s Vulnerability Reward Program does not provide explicit or clear language as to the scope of authorization. Largely one of the more notorious bug bounty programs, Google’s Vulnerability Reward Program has been in existence since 2010. Known for its higher payouts, hackers have been turning out in large numbers. Security exploits have ranged from getting control of a Google server by “playing with Google Calendar . . . to getting admin privileges on all blogs at Blogger.com,” none of which required sophisticated root kits or Unix scripts to find. While the scope of access for testing for security vulnerabilities includes “any Google-operated web service that handles reasonably sensitive user data” included on the list, the rules state that “this includes virtually all the content.” The use of “virtually all” indicates that not all the content is of authorized access and the rules do not go on to delineate clearly what content is unauthorized. that “[the] Combining the above ambiguous

91. Mills, supra note 90.
94. Id.
96. Vulnerability Reward Program, supra note 93.
terms with the fact that the program also requires that “testing must not violate any law, or disrupt or compromise any data that is not your own.” Grey hat hackers participating in Google’s Vulnerability Reward Program face a significant risk of violating the CFAA with each test they run.

PayPal’s program likewise contains contractual language that does not guarantee protection for criminal liability under the CFAA. PayPal’s program reassures participant that “if we conclude, in our sole discretion, that a disclosure respects and meets all the guidelines outlined below - we will not bring a private action or refer a matter for public inquiry.” Naturally, grey hats rely on the above statement in the listed rules as a manifestation of legal authorization via an express or implicit contract to test the site beyond normal permissions for security flaws. However, at the end of the document, the PayPal program includes a clause stating that the submitter “waives all other claims of any nature, including express contract, implied-in-fact contract, or quasi-contract, arising out of any disclosure of the Submission to eBay.” Claims of “any nature” arguably include consent to trespass, which is essentially nullified by the clause in dispute.

Even if the terms of a bug bounty program incorporate perfect contractual language, not every company or vendor on the Internet participates in bug bounty programs. For every bug bounty program, thousands of other corporations function online without one, leaving security weaknesses at the mercy of the Internet. Although the various bug bounty initiatives in the private sector take a step in the right direction through recognizing a legitimate role for grey hats in the security field, a policy approach is an eventual necessity in further incentivizing participation by grey hats and deriving the maximum social benefits from the grey hat community.

V. UPDATING THE CFAA

The modern interplay of malicious cyber activity and the Internet indicates a need to reconcile the realities of hacking with the needs of consumers and corporations. When Fortune 500 companies and entire governments cannot keep data private or protected from variant cyber threats, necessity entails a clear exemption in the CFAA to legitimize certain “whistle-blowing” activities in light of inherent security flaws. Any Congressional action to reform the CFAA should attempt to correct the over-breadth in the CFAA and establish a safe-harbor provision for members of the grey hat hacking community.

97. Id.
99. Id.
101. See supra note 98.
A. Redefining “Authorization”

While the CFAA imposes civil and criminal liability for accessing a protected computer “without” or “in excess of” authorization,102 the CFAA fails to define “authorization” per the statute and produces an unavoidably vague parameter of the precise activities that are punishable by law. In fact, since 2010, at least four federal circuit courts issued rulings where a defendant’s criminal liability hinged on the interpretation of “exceeds authorized access” in the CFAA.103 The result, is that private corporations effectively now decide what conduct violates federal criminal law when writing their use policies or terms of service. This over-breadth of the CFAA incurred by a lack of definition is the main point of contention for grey hats (and white hats), especially in light of the recent Auernheimer verdict. In order to begin reconciling the CFAA with cyberspace reality, the definition of “authorization” needs to take into consideration scenarios such as Auernheimer, where the public was free to access the unencrypted data (regardless of whether or not that was the intent of the vendor).

Following in the tradition of viewing Internet issues through the lens of property law, situations where the public accesses what should be restricted information is best analogized to a property owner leaving open a gate to their premises. From the perspective of a reasonable person, the vendor would keep the gate shut if the vendor did not want people walking onto the property. Absent any sort of “No Trespassing” sign or other form of notice, a reasonable person would not realize they were committing an act of trespass by merely walking through the gate.104 Therefore, leaving sensitive data open to the public in many ways creates an implied license. Under the Restatement (Second) of Torts, “acts or even [his] inaction may manifest a consent that will justify the other in acting in reliance upon them.”105 When “acts or silence and inaction, would be understood by a reasonable person as intended to indicate consent,” they “[manifest] apparent consent”106 and give rise to an implied license. Although situations where vendors leave data completely unencrypted and easily available to the public, such as in Auernheimer, remain rare, implied license via an open gate is equally unlikely to happen. Nonetheless, such situations are part of the cyber space reality and the CFAA needs to be constrained so as to not penalize reasonable intrusions through grey hacking or otherwise.

103. United States v. Nosal, 642 F.3d 781 (9th Cir.), reh’g granted en banc, 661 F.3d 1180 (9th Cir. 2011); United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010); United States v. John, 597 F.3d 263 (5th Cir. 2010); United States v. Auernheimer, No. 13-1816 (3rd Cir. April 11, 2014).
104. People v. Scott, 593 N.E.2d 1328 (N.Y. 1992) (“We hold that where landowners fence or post ‘No Trespassing’ signs on their private property or, by some other means, indicate unmistakably that entry is not permitted, the expectation that their privacy rights will be respected and that they will be free from unwanted intrusions is reasonable.”).
106. Id.
B. Safe-Harbor Provision for Grey Hat Hacking

In addition to constraining the language of the CFAA, lawmakers need to establish a safe-harbor provision for grey hats, so that this sub-group of the hacking community may research and report vulnerabilities without fear of legal repercussion. Again keeping in the tradition of interpreting Internet activities within the bounds of property law, a safe harbor provision would act like a specific exception or limited form of agency by permitting grey hats to trespass under certain guidelines and with limitations. Any provision must ensure that grey hats do not violate the privacy expectations of consumers more than otherwise required to protect such private information from malicious computer activity by black hats.

One model safe harbor provision might entail no jail time or charges if the grey hat notifies the vendor within 24-48 hours upon discovering the security flaw and the grey hat takes reasonable measures to put the vendor on notice. During this timeframe, the grey hat cannot take any action. In a week’s time (or some other reasonable time period), if the vendor does not respond and fails to notify consumers or does not respond to the grey hat with details as to how the vendor will proceed to secure the vulnerabilities, then the grey hat may announce the security flaw on a public forum. This model reconciles concerns between hackers and vendors alike: allowing vendors an opportunity to fix the vulnerability before it goes public and ensuring the grey hat community legal protection for reporting when vendors fail to repair the harms.

However, in order for the safe harbor provisions to be effective, grey hats must feel inclined to follow the new protocol. If the grey hat community perceives that vendors are not being held liable for breaches or taking too long to repair the security flaws, the grey hat community may end up by-passing the vendor once again. As emphasized in Part One of this paper, the law-abiding white hat hackers and the grey hats generally split on the manner of notice, with grey hats favoring notice in the form of public forums and news media. This division within hacking community is based largely on the failure of vendors to not only respond when put on notice of security breaches, but also on the near-absence of vendor liability. Indeed, liability, for the most part, depends on state legislatures, and thus varies from jurisdiction to jurisdiction and complicates the rule of law in a borderless cyberspace. In the absence of effective legal incentives to secure sensitive data, companies will continue to focus on their bottom line. Due to the transnational nature of the Internet, the federal government should step in and arrange more direct and nation-wide oversight that encourages data security liability on the part of companies that do not adequately protect the information they maintain. Specifically, rather than create an all new agency or data breach law, monitoring and enforcement of data

security should be directed through the already existing Federal Trade Commission ("FTC") under Section 5 of the Federal Trade Commission Act.

Per Section 5 of the Federal Trade Commission Act ("Act"), the FTC has taken action against companies that failed to implement reasonable security measures to protect customers' personal information.\(^{108}\) Section 5 of the Act prohibits unfair or deceptive acts or practices in or affecting commerce that cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumers nor offset by countervailing benefits to consumers or competition."\(^{109}\) Although Section 5 states "an actual breach of security is not a prerequisite for enforcement,"\(^{110}\) the FTC has only targeted companies that had some kind of actual security failure or have intentionally violated their privacy policies.\(^{111}\) To date, each company formerly subject to an FTC complaint for unfair or deceptive trade practices related to consumer privacy settled, rather than fully litigated, the claim.\(^{112}\) In turn, no court has yet affirmed the FTC's application of Section 5. Furthermore, while the FTC may bring actions against these companies, procedural rules that limit FTC court wins to disgorgement of improper profits, rather than civil penalties, severely hinder the FTC's ability to win civil penalties.\(^{113}\) One possible policy solution would be an Act of Congress encouraging the FTC to seek monetary penalties of this sort, as well as the creation of a computer security equivalent to the National Traffic and Motor Vehicle Safety Act\(^{114}\) that would grant the FTC enforcement powers.

Drawing on the National Traffic and Motor Vehicle Safety Act, Congress should authorize the FTC to issue computer security standards and notify customers of security risks. The National Traffic and Motor Vehicle Safety Act gives the Department of Transportation's National Highway Traffic Safety Administration (NHTSA) power to issue vehicle safety standards and to require manufacturers to recall vehicles that have safety-related defects or do not meet

\(^{108}\) 15 U.S.C. §§ 45 (2006). (Section 5 of the Federal Trade Commission Act grants the FTC the power to take enforcement actions against persons, partnerships, or corporations, but not certain financial institutions, for engaging in unfair or deceptive trade practices. Such practices include those that cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumers nor offset by countervailing benefits to consumers or competition.).
\(^{109}\) Id.
\(^{110}\) Id.
\(^{111}\) The Federal Trade Commission’s Section 5 privacy cases can be viewed at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html. As of January 31, 2014, the FTC has brought at least 51 legal actions against organizations that have violated consumers’ privacy rights, or misled them by failing to maintain security for sensitive consumer information.
\(^{112}\) Id.
\(^{113}\) 15 U.S.C. § 57b(b) (2009) (limiting the FTC only to equitable remedies, such as disgorgement of improper profits by corporate wrongdoers, which often does not apply in the case of companies that have been the subject of data breach, unless that company operated in collusion with the person stealing the information).
Federal safety standards.115 Although many manufacturers voluntarily initiate recalls on their own, other members of the automotive industry require extra incentive through either NHTSA investigations or NHTSA orders via the courts.116 The NHTSA came about after public outcry in the mid-1960s to increase the safety of cars following the publication of two key pieces of literature: Unsafe at Any Speed, by Ralph Nader, and the National Academy of Sciences’ “Accidental Death and Disability—The Neglected Disease of Modern Society.”117 Like the great roads linking commerce around the nation, the Internet links commerce from corner to corner of the United States. Everyday, Consumers in sizable amounts travel and interact along the appropriately named “information super highway”. While not immediately so traumatic (or violent) as a traffic accident, the security of our online infrastructure is one of national security concern118 and the effects of private consumer data breaches (with or without any information stolen) can turn the lives of consumers upside down.119 Monetary, dignitary, and actual harms all spill-over from cyberspace and into our Internet-omnipresent lives. Such a threat of harm invites Congressional intervention and regulation.

Further, in following the Department of Transportation’s approach to NHTSA, the FTC could form a new bureau to oversee the requirements of a computer security act or hand oversight to the Consumer Affairs Bureau. As with the NHTSA, many vendors will voluntarily initiate security provisions, whereas others will require a court order or FTC investigation. Regarding security risks

discovered by the vendor or a grey hat, the FTC may choose to mandate a notice requirement for vendors. One approach would require vendors, following the discovery of a security risk by a third-party, to notify the FTC within one week (or other reasonable time period determined by Congress or the FTC). Otherwise, the party that discovered the vulnerability may contact the FTC and go public with the information. Additionally, the vendor would then be required to remedy the problem at no charge to consumers. Alternatively, due to the deeply-ingrained aversion by grey hats to working directly with vendors, another model might allow grey hats to directly and anonymously contact the FTC, who would then follow up with the vendor within 48 hours and, in doing so, place the vendor on notice. Following notice, the FTC would be responsible for monitoring the vendor’s corrective action to ensure successful completion of the patch deployment (or other necessary remedial measure).

The reporting mechanism of a computer security safety act and a coinciding agency for monitoring remedial measures strikes a balance between grey hats and vendors, while simultaneously recognizing the value and risk to consumer data on computer networks. Admittedly relating computer security flaws to vehicle defects is an imperfect analogy, but websites and software are still products and a measure of consumer protection is needed in this day and age. Without oversight of vendor response to security flaws, the likelihood of the status quo will remain constant; many vulnerabilities will not be remedied or deployed in a timely fashion (if at all).

VI. CONCLUSION

Scholars, government officials, journalists, and computer scientists are in concurrence that inadequate security is an emerging threat, possibly even a catastrophic one. However, computer security will always be flawed and, as long as there are hackers, those security holes will be exploited. A software or hardware vendor can neither fix a problem they don’t know about nor fully anticipate and protect against all possible cyber attacks. The question is then just whom do vendors want to exploit those security vulnerabilities: the grey hat or the black hat?

Recent breaches illustrate the increasingly transnational nature of cyber crime. From the development of the program to the dissemination of the data to other countries following a breach, cyber crimes often times involve multiple nation states. For instance, in the 2013 Target data breach, U.S. authorities implicated citizens of Mexico in mining the data, while the program used to

\[120. \text{See Derek E. Bambauer, } \textit{Conundrum}, \textit{96 MINN. L. REV.} 584, 588 (2011).\]
DID THE NATIONAL SECURITY AGENCY DESTROY THE PROSPECTS FOR CONFIDENTIALITY AND PRIVILEGE WHEN LAWYERS STORE CLIENTS’ FILES IN THE CLOUD – AND WHAT, IF ANYTHING, CAN LAWYERS AND LAW FIRMS REALISTICALLY DO IN RESPONSE?

Sarah Jane Hughes*

I. INTRODUCTION

In the months since Edward Snowden’s revelations about the National Security Agency’s (“NSA”) comprehensive gathering of metadata from telephone calls, emails and uses of the Internet here and abroad, many commentators have focused on whether and to what extent the data collection programs have exceeded the NSA’s authority.1 Additionally, commentators have asked how the data may have enabled the NSA’s recognition of many relationships previously considered confidential by the parties to the underlying communications.

* Sarah Jane Hughes is the University Scholar and Fellow in Commercial Law, Maurer School of Law, Indiana University, Bloomington, Indiana. Hughes is the co-author of Responding to National Security Letters: A Practitioner’s Guide (ABA, 2009) (with Professor David P. Fidler), the curator and primary editor of RFIDS, Near-Field Communications and Mobile Payments: A Guide for Lawyers (ABA, 2013), and co-author with Roland T. Trope of the article entitled Red Skies in the Morning – Professional Ethics at the Dawn of Cloud Computing, 38 Wm. Mitchell L. Rev. 111 (2011), hard copies of which are available from the author. She also has published articles on privacy and data security, electronic and mobile payments, banking law, virtual currencies, and policies and regulations related to the deterrence of money laundering. She is a graduate of Mount Holyoke College and of the University of Washington’s School of Law. She can be reached at sjhughes@indiana.edu.

Professor Hughes wishes to thank Professor Jon Garon for his kind invitation to participate in this Law + Informatics Symposium on Cyber Defense Strategies and Responsibilities for Business and Industry. She also acknowledges the valuable research for this paper provided to her by Janelle R. Duyck, Maurer School Class of 2015, particularly the compilation of formal and informal opinions issued by state bar associations or states’ highest courts on cloud-computing and professional ethics since August 4, 2011 that appears as Appendix I to this paper.

This paper would not be possible without the path-breaking presentations in 2009 and 2010 by Roland L. Trope and Claudia Ray, members of the New York Bar, relating to professional ethics and use of social media and cloud computing entitled The Real Realities of Cloud Computing: Ethical Issues for Lawyers, Law Firms and Judges, Essay for CLE Program, ABA Annual Meeting, San Francisco, August 2010, and Head in the Cloud – Feet on the Ground: Understanding the Ethical Challenges of Web 2.0 for Lawyers, Law Firms and Judges, ABA Annual Meeting, Chicago, August 2009. Copies of the essays Mr. Trope and Ms. Ray prepared are on file with the author.

Less attention had been paid to other collateral consequences of the NSA’s data-gathering work and the threats it poses to the confidential and privileged information that communications between lawyers and clients often contain. Focus shifted to certain collateral consequences with two relatively recent revelations in particular: the revelations that (1) the NSA may have introduced some tools to allow it to decrypt encrypted data, and (2) that it apparently enjoyed the fruits of signals intelligence by its Australian counterpart, the Australian Signals Directorate, relating to the representation by a U.S. law firm and its client the government of Indonesia pertaining to a then-pending trade dispute between the U.S. and Indonesia, and shared those fruits with client agencies in the federal government. Both reports raise fresh concerns over privileged communications and clients’ confidential data moving through electronic communications into storage, including cloud computing storage.

In our 2011 article entitled Red Skies in the Morning – Professional Ethics at the Dawn of Cloud Computing [hereinafter “Red Skies”], Roland L. Trope and I observed, among other things, that lawyers and law firms using the cloud for storage of clients’ files and documents would enable easier access to files and documents by governments. We asserted that lawyers, law firms, and clients would not know about the access or manner of access until the access had been obtained. (Like most Americans, at that time, we were unaware of the scope of the NSA’s surveillance programs relating to domestic telecom communications and Internet storage.) Our prediction was based on the then-known authority for the government to gain access, the ongoing disputes about the protections that the Electronic Privacy Communications Act of 1986 (“ECPA”) gave to telecom records, and the fact that both the Foreign Intelligence Supervision Act (“FISA”) and other “national security letters” authority prohibited the disclosure


5. Id. at 230-233.

6. Id.


of their receipt by the person or firm holding the information sought. Only in recent months has the Department of Justice made it clear that they obtained information used in criminal proceedings via one of the “national security” avenues of access they have.

Our 2011 article also anticipated the enhanced risks that governments and others could gain access to cloud-stored files when the cloud provider stores documents in undisclosed offshore locations, and we cited the ABA’s Formal Op. 08-451, which noted that new issues could arise with the non-U.S. laws on seizures in judicial or administrative proceedings notwithstanding claims of client confidentiality.

This paper updates that 2011 article in modest ways related to its forecast of more and easier government surveillance of work product and client documents in cloud storage. From the base of the 2011 article, it also looks at the more recent past with its revelations of NSA surveillance and towards a future in which lawyers and law firms may have to employ less technologically hip techniques for communicating with clients while maintaining traditional lawyer-client privileges and storing clients’ trade secrets and other confidential records.

Part II of this article explains the most current rules on lawyers’ obligations to protect the confidential and privileged information they obtain from clients using as its benchmarks the August 2012 amendment to Rules 1.1, 1.4, 1.6, and 1.15, and new comments to those sections of the America Bar Association’s (ABA) Model Rules of Professional Conduct (“MRPC”) based on the ABA’s Commission on Ethics 20/20. It also compares the 2012 amendments to the Model Rules of Professional Conduct that relate to the NSA data-collection programs to the prior MRPC versions of these

10. 18 U.S.C. § 2709 (2011); 18 U.S.C. § 3123(d)(2) (2011); see also Matt Apuzzo & Nicole Perlroth, U.S. relaxes some data disclosure rules, N.Y. TIMES, Jan 28, 2014, at B1-2 (providing that earlier in 2014, the Obama administration agreed to allow Internet companies such as Google, Microsoft, Yahoo, and Facebook to disclose how often the government asks for their customers’ information, but will not permit the companies to reveal what the government collects or how much data it collects. Apuzzo and Perlroth also cite Forrester Research predictions that concerns over data accessed by national security letters and FISA court orders “could cost the so-called cloud computing industry as much as $180 billion – a quarter of its revenues – by 2016”).


13. See id.


16. MODEL RULES OF PROF’L CONDUCT R. 1.6 (2012).


Rules. To provide additional perspective on access to files and documents stored in the cloud by federal and state law enforcement agencies in the United States other than the intelligence agencies, this article briefly discusses the ABA’s 2012 Criminal Justice Standards on Law Enforcement Access to Third Party Records.

Part III looks at the differences between “privileged” and “confidential” information and the risks to each category of information that the NSA surveillance raises. Part IV discusses enhanced risks to data and storage flowing from the formerly secret “back doors” and encryption-breaking practices that NSA has introduced into commonly used electronics such as tablets and smart phones that allows more surveillance by the NSA and FBI, and hacking by many potential sources including possibly by clients’ counter-parties. This part expresses doubts that President Obama’s January 17, 2014 Signals Intelligence Directive, which outlines the scope of continuing collection and review of telephonic and other electronic communications, will correct the risks to clients’ confidential and privileged records in the cloud.

In Part V, this article briefly discusses lawyers’ and law firms’ duties arising under data security breach notification laws enacted by the States and in the European Union that arise when their electronic records are hacked, whether in their own offices or in the cloud. Among the sources of data security prevention and public responsibility for breaches and notification, it also cites the Federal Trade Commission Act.

19. See Trope & Hughes, supra note 4, for a fulsome discussion of the pre-2012 version of the Model Rules of Professional Conduct.


21. See Close the N.S.A.’s Back Doors, N.Y. TIMES, Sept. 22, 2013, at SR10, available at http://www.nytimes.com/2013/09/22/opinion/sunday/close-the-nsas-back-doors.html?_r=0, (mentioning coverage by itself, The Guardian, and ProPublica that the NSA “now has access to the codes that protect commerce and banking systems, trade secrets and medical records, and everyone’s e-mail and Internet chat messages, including virtual private networks, and encryption protecting data on iPhone, Android and BlackBerry phones”).

22. See, e.g., E. Michael Maloof, NSA Has Total Access via Microsoft Windows, http://www.wnd.com/2013/06/nsa-has-total-access-via-microsoft-windows/ (last visited Apr. 14, 2014) (citing Joseph Farah, G2 Bulletin, http://g2.wnd.com (Jun. 23, 2013)) (reporting that the NSA has “backdoor access to all Windows software since the release of Windows 95” and tying the backdoors to “insistence by the agency and federal law enforcement for backdoor “keys” to any encryption; providing further that Windows “software driver used for security and encryption functions contains unusual features that give the NSA the backdoor access” and “[s]uch access to the encryption system of Windows can allow NSA to compromise a person’s entire operating system”).


Part VI first surveys recent, publicly available advice, primarily concerning technology tools that address cloud computing risks and solutions. It also reports on increasing client demands that law firms undergo cybersecurity audits themselves, and states some conclusions about lawyers’ obligations when using cloud computing and storage, including new risks connected to the NSA’s telecommunications data-gathering programs and its back-doors and encryption-busting propensities that threaten lawyers’ ability to use the cloud for storage of confidential or privileged communications with and information belonging to clients as to require prompt reexamination of such use and renewed efforts to inform clients of the potential risks.25

In Part VII, this article poses some questions about the future of protecting clients’ trade secrets and other highly proprietary information from government surveillance and via back doors from competitors’ or other hackers’ intrusions. Risks to confidential and privileged data point to the need for some restraint, if technologically feasible, on collection by the NSA, FBI and other agencies, of communications involving lawyers and law firms with clouds. Alternatively, risks point to a need for post-collection minimization policies that federal agencies ought to implement or be forced to implement by the Obama Administration or Congress. This part recommends that lawyers and law firms may have no alternative but to revert to relatively old-fashioned approaches to protecting clients’ data that is confidential or privileged despite the efficiency and economy of the cloud. These methods include in-person conversations, physical storage of tangible records with proper physical and administrative safeguards in place to protect them – as well as a really good map of where the records are stored, and such old-fashioned ideas as using manual typewriters for the most sensitive communications, such as clients’ patent applications and merger and acquisition plans.

II. THE 2012 AMENDMENTS TO THE MODEL RULES OF PROFESSIONAL CONDUCT

Our 2011 Red Skies article included extensive analysis of core duties included in the 2007 version of the MRPC,26 particularly, the duties to:

- provide competent representation and, accordingly, to stay abreast of new technologies and uses of technologies;27

- obtain clients’ informed consent to the use of cloud storage for communications with and documents belonging to clients, including attorney work-product on client matters;28

25. MODEL RULES OF PROF’L CONDUCT R. 1.6 (2007).
26. Trope & Hughes, supra note 4 at 137-63.
27. Infra at text accompanying notes 57 to 96.
protect confidential information and privileged communications from “inadvertent disclosure of, or unauthorized access to, information relating to the representation of a client” by use of reasonable efforts. And,

• communicate with clients on various aspects of the representation.

Amendments to the main text or to the comments accompanying the MRPC incorporated in the 2012 amendments to the MRPC adjust some of the duties.

A. Rule 1.1 Competence

In Red Skies, Mr. Trope and I argued that Rule 1.1’s mandate for “competent representation” included a duty to stay abreast of new technologies and of risks related to the use of technologies. New Comment [6] to MRPC 1.1 now mentions those duties explicitly:

[6] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

B. Rule 1.4 Communication

Rule 1.4 was not amended by the American Bar Association in 2012. It still reads:

(a) A lawyer shall:

(1) promptly inform the client of any decision or circumstance with respect to which the client’s informed consent, as defined in Rule 1.0(e), is required by these Rules;

28. *Infra* at text accompanying notes 97 to 138.
32. Trope & Hughes, *supra* note 4 at 154.
33. MODEL RULES OF PROF’L CONDUCT R. 1.1, cmt. 6 (2012) (underlining in original demonstrates changes from the 2007 text).
(2) consult with the client about the means by which the client’s objectives are to be accomplished;

(3) reasonably keep the client informed about the status of the matter;

(4) promptly comply with reasonable requests for information; and

(5) consult with the client about any relevant limitation on the lawyer’s conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.34

Comment [4] to MRPC 1.4 also was amended in 2012,35 but not, in my view, in a manner that alters the recommendations that Mr. Trope and I made in Red Skies.36

Comment 16 to MRPC 1.6 requires lawyers to recognize the risks that technology poses, particularly where a third party might have access to the information.37 Our 2011 article concluded that “… in addition to recognizing risks, to competently safeguard information, the lawyer must similarly assume and provide for the fact that third-party communications providers are not likely to protect client information as zealously as the client’s advocate should.”38

Rule 1.6 Confidentiality of Information now reads:

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

35. MODEL RULES OF PROF’L CONDUCT R. 1.4, cmt. 4 (2012) (“Client telephone calls should be promptly returned or acknowledged,” was replaced by “[A] lawyer should promptly respond to or acknowledge client communications.”).
36. Trope & Hughes, supra note 4 at 137-51.
37. MODEL RULES OF PROF’L CONDUCT R. 1.6, cmt. 16 (2007). See also ABA Formal Op. 08-451, supra note 12 (concluding that a lawyer may outsource support services, but recognizing that the lawyer ultimately remains responsible for rendering competent legal services to the client).
(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to prevent reasonably certain death or substantial bodily harm;

(2) to prevent the client from committing a crime or fraud that is reasonably to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer’s services;

(3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client’s commission of a crime or fraud in furtherance of which the client has used the lawyer’s services;

(4) to secure legal advice about the lawyer’s compliance with these Rules;

(5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer’s representation of the client; or

(6) to comply with other law or a court order.

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.  

I would make two observations in particular about MRPC 1.6. First, Rule 1.6(a) does not contain a qualifying subjective mental element, which its 2007 predecessor also lacked. The continued absence of a “knowing” requirement in Rule 1.6(a) means that, absent informed consent, the lawyer shall not reveal information relating to the representation.

Second, new MRPC Rule 1.6 (c) creates a duty that requires lawyers to recognize the issues related to drafts stored in the cloud. These issues include, at the minimum, prospects that (1) copies of all documents are made each time that a document is moved to the cloud, and (2) standard cloud storage protocols use

39. MODEL RULES OF PROF’L CONDUCT R. 1.6 (2012).
40. MODEL RULES OF PROF’L CONDUCT R. 1.6 (2012).
41. Trope & Hughes, supra note 4, at 152.
back-up storage of multiple copies of documents. Regrettably, lawyers may have no knowledge, at any given time, how many copies of a file exist and where those copies may be stored. Copies effectively are all individual documents for purposes of e-discovery, whether or not the lawyer or firm knows of their existence. Copies also potentially “reside” in different jurisdictions or nations (where privacy and security laws may demand different protections, including no protection at all for data originating outside their borders). Copies also may become unavailable via outages to the cloud servers at critical moments with no indemnification or reimbursement for associated injuries likely forthcoming from the cloud providers.

These facts complicate the lawyer’s ability to recognize and control risks to clients’ confidential and privileged documents and communications.

The Rule also appears to require awareness and, to the extent feasible, prevention of newer-age risks in choosing to store data in the cloud including both the risk of surveillance by government agencies in the U.S. and abroad and risks of non-government penetration via the “back doors” introduced into certain electronic devices by U.S. agencies. Given what we now know of the NSA’s practices both alone and in collaboration with friendly intelligence services, prevention could require abandonment of many technologically enabled efficiencies – such as conference calls or Skype calls in lieu of travel or of cloud-shared work products – in favor of old-fashioned communications and storage methods mentioned in Part VII of this article.

Accompanying new Rule 1.6(c) are amendments of comments [18] and [19]. Comment [18] to Rule 1.6(c) now provides:

C. Acting Competently to Preserve Confidentiality

Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are...

42. Trope & Hughes, supra note 4, at 224-230.
43. Id. at 175-199 (discussion including provisions of cloud contracts on liability to their clients).
46. See Risen & Poitras, supra note 2.
47. MODEL RULES OF PROF’L CONDUCT R. 1.6(c), cmt. 18-19 (2012).
participating in the representation of the client or who are subject to the lawyer’s supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer’s efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forego security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client’s information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements on loss of, or unauthorized access to, electronic information is beyond the scope of these Rules. For a lawyer’s duties when sharing information with nonlawyers outside the lawyer’s own law firm, see Rule 5.3, Comments [3]-[4].48

New comment [19] to Rule 1.6(c) adds the last sentence to what had been in the 2007 comment:

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer’s expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to

---

48. MODEL RULES OF PROF’L CONDUCT R. 1.6(c), cmt. 18 (2012) (underlining original in published text of amended comment 19).
comply with other law, such as state or federal laws that govern data privacy, is beyond the scope of these Rules.\textsuperscript{49}

The 2012 amendments also remind lawyers and law firms of their duties to protect documents and data covered by confidentiality or privilege rules that belong to former clients:

**Former Client**

[20] The duty of confidentiality continues after the client-lawyer relationship has terminated. See Rule 1.9(c)(2). See Rule 1.9(c)(1) for the prohibition against using such information to the disadvantage of the former client.\textsuperscript{50}

Accordingly, lawyers’ and law firms’ duties to files, documents, data and communications extend beyond the representation and concerns over cloud storage apply to information archived in the cloud, to the same extent as they apply to active files and clients.

Based on the information that the NSA’s surveillance of electronic communications has been ongoing for many years, it appears that files that lawyers and law firms archived in the past could be imperiled as well as more recently stored files.

**D. Rule 1.15 Safekeeping Property**

Finally, lawyers’ duties to protect clients’ property are based on Rule 1.15.\textsuperscript{51} Subsection 1.15(a), among other things, provides that “... Other property shall be identified as such and appropriately safeguarded.”\textsuperscript{52} The duty to safeguard property “appropriately” is the key aspect of this Rule’s relationship to cloud computing and other technology uses by lawyers and law firms for the purpose of this article.

In Red Skies, Mr. Trope and I pointed out that outages in the cloud can render stored files unavailable for periods of time while the cloud provider recovers data, etc.\textsuperscript{53} We also explained that lawyers and law firms can lose access to cloud-stored data by breaching their contracts with cloud providers.\textsuperscript{54} Thus, the risk of losing access to documents temporarily or perhaps permanently in the event of a more massive cloud outage or dispute between the lawyer or firm and the provider should be considered when lawyers decide whether to store clients’ most valuable documents in the cloud and in their choice of cloud providers.

\textsuperscript{49} Model Rules of Prof’l Conduct R. 1.6(c), cmt. 18 (2012) (underlining original in published text of new comment 18).
\textsuperscript{50} Model Rules of Prof’l Conduct R. 1.6, cmt. 20 (2012).
\textsuperscript{51} Model Rules of Prof’l Conduct R. 1.15 (2012).
\textsuperscript{52} Id.
\textsuperscript{53} Trope & Hughes, supra note 4, at 175-199.
\textsuperscript{54} Id. at 196-198.
This consideration is more important if the only or most recent copies are stored in the cloud, as a recent episode in North Carolina revealed. According to media reports, a Charlotte law firm suffered the loss of access to “its entire cache of legal documents to the malware program called ‘Cryptolocker Trojan’” despite attempts by the principals to pay the $300 ransom the hackers demanded in a bid to have the documents unscrambled. At least, according to the report, the malware only destroyed the ability to read the contents of the stored files, it apparently did not steal them. However, this may be of less comfort to the firm because, assuming that the firm was entirely “paperless” as many strive to be, the firm lost documents of value to its clients and to its relationship with clients.

III. DID NSA DATA CAPTURE DESTROY ATTORNEY-CLIENT PRIVILEGE OR WAIVE CONFIDENTIALITY STATUS FOR CLIENTS’ FILES AND DATA THAT LAWYERS AND LAW FIRMS STORED IN THE CLOUD?

In this part of the article, we come to the heart of concerns that explicitly relate to surveillance of communications, including telephonic and transmissions to cloud storage of files that lawyers hold or work on with clients. Privilege and confidentiality are separate concepts and will be discussed in turn below.

A. Attorney-Client Privilege and NSA Surveillance

According to a leading commentator on the attorney-client privilege, Professor Geoffrey C. Hazard, Jr.:

The attorney-client privilege may well be the pivotal element of the modern American lawyer’s professional functions. It is considered indispensable to the lawyer’s function as advocate on the theory that the advocate can adequately prepare a case only if the client is free to disclose everything, bad as well as good. The privilege is also considered necessary to the function as confidential counselor in law on the similar theory that the legal counselor can properly advise the client what to do only if the client is free to make full disclosure.

But Professor Hazard also observed that attorney-client privilege “is invoked to conceal legally dubious or dirty business. And when dubious or dirty business has been done, most likely someone has suffered as a result. In the nature of things, then the attorney-client privilege has its victims.” Moreover, he suggested:

56. See id.
58. Id. at 1062.
In the present-day law [circa 1978], the issue concerning the attorney-client privilege is not whether it should exist, but precisely what its terms should be. There is no responsible opinion suggesting that the privilege be completely abolished. Total abolition would mean that an accused in a criminal case could not explain his version of the matter to his lawyer without its being transmitted to the prosecution. Defense counsel would become a medium of confession, a result that would substantially impair both the accused’s right to counsel and the privilege against self-incrimination. Hence, it is common ground that the privilege ought to apply at least to communications by an accused criminal to his counsel, in contemplation of defense of a pending or imminently threatened prosecution, concerning a completed crime. Beyond this there is controversy as to the proper scope of the privilege, although superficially the authorities are in substantial agreement. 59

Against this backdrop, we have evidence of one of the most bizarre examples of surveillance of lawyer-client communications that has come to light recently. I speak of reports published in early 2014 that via its Australian counterpart, the Australian Signals Directorate, the Directorate received and shared with the NSA the fact of communications between the DC office of a major U.S.-based law firm and its client, the government of Indonesia, related to a trade dispute between the two governments. 60 Apparently, not only did the Signals Directorate pass the communications – so far unspecified in their form – to the NSA, the NSA reputed shared the communications with “a client,” whose identity one can infer was the White House, Department of Commerce, or the Office of the U.S. Trade Representative, the counter-party in the trade dispute. 61

There is a bit of good news that follows the revelations about capture of the communications between Mayer Brown, the firm reportedly involved, and its client. Following publication of the story, I discussed it with several faculty colleagues to obtain their sense of the damage to a client’s actual privileged communications with its lawyer. Here is how one senior colleague responded:

A privilege is personal property. It belongs to the person/corporation that made the communication. The person must have intended it to be confidential forever, and it must have been confidential in fact. Only the behavior of the holder of the privilege or their agents can waive it, expressly or implicitly or sometimes negligently. Therefore, in most jurisdictions, intercepted

59. Id. at 1062-1063. As background for the balance of his argument, Professor Hazard also cited Uniform Rules of Evidence Rule 26, the ALI Model Code of Evidence rule 212 (1942), and Proposed Federal Rules of Evidence rule 502, 51 F.R.D. 315 (1971). Uniform Rules of Evidence rule 26, at that time, provided that the lawyer-client privilege applies to “communications … between lawyer and his client in the course of that relationship and in professional confidence … unless the legal service was sought or obtained to commit or plan to commit a crime or tort.” Hazard, supra note 56, at 1063, citing Uniform Rules of Evidence rule 26.

60. Risen & Poitras, supra note 3.

61. Id.
communications, even under warrant, are still privileged. But that only means that they cannot be used in court proceedings. If the information is communicated voluntarily or knowingly to a third party with whom the speaker does not have an independent privileged relationship, it is no longer privileged, although it may still be confidential for various regulatory purposes. 62

A second colleague added the following useful perspective, among others:

. . . When the NSA surrepticiously intercepts communications, this is not the kind of context in which a party purposefully or intentionally waives the confidentiality of their communication. Therefore, as a doctrinal matter, the notion of “waiver” should not be extended to apply to communications surrepticiously intercepted by the government. As well, from a practical and a policy perspective, the opposite rule would allow the government to intercept confidential communications – even in cases between plaintiffs and the government – and then argue that confidential attorney-client communications are not protected by attorney-client privilege. This seems problematic for a number of reasons. 63

I asked a third colleague and he responded:

. . . I think the federal approach is that where the law does not prohibit intrusion into a FISA A-C communication, the government nevertheless must take reasonable steps to protect any information collected, shared, etc. If there are Attorney General procedures on this topic it would be valuable to have the professional community review, comment, and advise on them. 64

Thus, it would appear that communications between lawyer and client intercepted by the NSA or received by the NSA and other U.S. agencies should be entitled to lawyer-privilege if the issue arises in a court proceeding. 65 But a different rule might apply – though also might not be applied – not if the issue arises in another forum, like negotiations over a trade dispute. And, certainly, in negotiations the privilege may be less important than the loss of confidentiality for the information intercepted as to data or strategy.

62. Email from Law Professor, Indiana University Maurer School of Law, to author (February 24, 2014) (on file with the author).
63. Email from a second Law Professor, Indiana University Maurer School of Law, to author (February 24, 2014) (on file with the author).
64. Email from a third Law Professor, Indiana University Maurer School of Law, to author (February 25, 2014) (on file with the author).
65. See supra note 62; see also supra note 63; see also supra note 64.
B. Confidentiality and Documents Stored in Clouds and, Presumably, Subjected to NSA Surveillance

The North Carolina law firm described above at least did not have their files stolen, just rendered unusable by everyone, including their clients. Although unusable, the confidentiality of the files was (apparently) not breached.

But let’s think about the other law firm whose communications and shared work products likely contained information about the trade dispute that the client government considered confidential. What happens now? Did the law firm violate the duty to keep clients’ confidential data confidential?

As explained above, the 2012 Model Rules of Professional Conduct impose on lawyers’ duties to keep clients’ confidential information confidential. This duty is explained, once again, in the following terms by new comment [19] to Rule 1.6(c):

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer’s expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state or federal laws that govern data privacy, is beyond the scope of these Rules.66

Presumably, before the 2013 Snowden releases about the scope of NSA’s interceptions, lawyers and law firms might not have imagined that their telephonic communications would be intercepted and digested – or that no court would authorize such interceptions in the context of a trade dispute.

But how about in this post-Snowden environment? There are two options, apparently. First, the client may require the lawyer to employ special security measures. Second, the client may give informed consent to the use of communications means that do not comply with the requirements of Rule 1.6. Either way, the lawyer and his or her clients must have conversations about the new risks to confidentiality that NSA interceptions now pose – and come to an

66. MODEL RULES OF PROF’L CONDUCT R. 1.6(c), comm. (2012) (underlining original in published text of new comment).
agreement about how the client wishes communications to be handled and protected. As described above, the client must make an informed consent – and this means that the lawyer knows enough about various technologies and the risks they may present to enable a frank and thorough conversation about the risks before the client makes its decision. It means that many more lawyers will have to learn a lot more about certain technologies and follow the literature and jurisprudence about NSA and other government interceptions than ever before.

IV. SHOULD REVELATIONS ABOUT THE NSA’S ACTIONS AFFECT LAWYERS’ USE OF CLOUD COMPUTING? WHAT LIMITS SHOULD BE PLACED ON FEDERAL AND STATE LAW ENFORCEMENT AGENCIES’ ACCESS TO CLIENTS’ DATA HELD BY LAWYERS AND LAW FIRMS IN CLOUDS?

Subpart A of this part briefly discusses enhanced risks to lawyers’ use of telecom and cloud computing and storage flowing from the secret “back doors” that the NSA secretly introduced into commonly used electronics such as tablets and smart phones. Subpart B introduces the 2012 American Bar Association Standards on Law Enforcement Access to Third Party Records.

A. NSA Data Mining

Commentators have assumed that the “back doors” that the NSA introduced into electronics were intended to allow more surveillance by the NSA and FBI. They also express concerns that the back doors enable hacking by many potential sources including possibly by clients’ counter-parties. The topic of demonstrating how data held by one government agency could be misused by hackers came up at a recent House Financial Services Committee hearing. During questioning about his agency’s collection of consumer credit transaction records, Director Richard Cordray of the Consumer Financial Protection Bureau responded that he could not guarantee their safety to 100%.

67. See, e.g., Maloof, supra note 22 (reporting that the NSA has “backdoor access to all Windows software since the release of Windows 95” and tying the backdoors to “insistence by the agency and federal law enforcement for backdoor ‘keys’ to any encryption.”).

68. Am. Bar Ass’n, supra note 20.

69. See Maloof, supra note 22.

70. Id. (report that the Windows “software driver used for security and encryption functions contains unusual features that give the NSA the backdoor access” and that “[s]uch access to the encryption system of Windows can allow NSA to compromise a person’s entire operating system”).

B. ABA Standards for Law Enforcement Access to Third Party Records

One area of risk to the confidentiality and privilege of clients’ documents and data that has been largely ignored since Edward Snowden’s revelations about the NSA data-collection practices relates to other, non-national security law enforcement agencies. These agencies might be interested in clients’ records and communications in connection with the prevention and investigation of crimes, including money laundering and tax evasion, completeness of responses to agencies’ investigations into compliance with federal securities or commodities or consumer credit or privacy protection laws, or for other investigatory purposes.

Agency interest in data stored with various institutional parties, including law firms, implicates the “third party records” doctrine that the United States Supreme Court articulated from the 1960’s to 1980’s. This doctrine has come under criticism since the advent of email, global positioning devices, social media, and cloud computing. The two primary Supreme Court decisions related to the “third-party-records” doctrine are United States v. Miller,72 and Smith v. Maryland.73

In response in part to growing concerns about telecommunications and other access to third-party records by all levels of government, the American Bar Association in 2012 updated its Standards for Law Enforcement Access to Third Party Records.74 Of particular relevance to the topic of this paper are Standards 25-4.1 (Categories of Information), 25-4.2 (Categories of Protection), and 25-5.3 (Requirements for Access to Records). These rules provide:

1. Standard 25-4.1 Categories of information

Types of information maintained by institutional third parties should be classified as highly private, moderately private, minimally private, or not private. In making that determination, a legislature, court, or administrative agency should consider present and developing technology and the extent to which:

(a) the initial transfer of such information to an institutional third party is reasonably necessary to participate meaningfully in society or in commerce, or is socially beneficial, including to freedom of speech and association;

72. 425 U.S. 435 (1976) (holding that no person should have a reasonable expectation of privacy in information they voluntarily conveyed to a third party).
73. 442 U.S. 735 (1979) (holding installation at telephone company offices and use of a pen register was not a “search” and required no warrant because the individual target of the pen register had no reasonable expectation of privacy in records at the telephone company offices).
(b) such information is personal, including the extent to which it is intimate and likely to cause embarrassment or stigma if disclosed, and whether outside of the initial transfer to an institutional third party it is typically disclosed only within one’s close social network, if at all;

(c) such information is accessible to and accessed by non-government persons outside the institutional third party; and

(d) existing law, including the law of privilege, restricts or allows access to and dissemination of such information or of comparable information.

2. Standard 25-4.2 Categories of protection

(a) The type of authorization required for obtaining a record should depend upon the privacy of the type of information in that record, such that: records containing highly private information should be highly protected, records containing moderately private information should be moderately protected, records containing minimally private information should be minimally protected, and records containing information that is not private should be unprotected. If a record contains different types of information, it should be afforded the level of protection appropriate for the most private type it contains.

(b) If the limitation imposed by subdivision (a) would render law enforcement unable to solve or prevent an unacceptable amount of otherwise solvable or preventable crime, such that the benefits of respecting privacy are outweighed by this social cost, a legislature may consider reducing, to the limited extent necessary to correct this imbalance, the level of protection for that type of information, so long as doing so does not violate the federal or applicable state constitution.

3. Standard 25-5.3 Requirements for access to records

(a) Absent more demanding constitutional protection, consent pursuant to Standard 25-5.1, and emergency aid and exigent circumstances pursuant to Standard 25-5.4; and consistent with the privilege requirements of Standard 5.3(c); law enforcement should be permitted to access a record maintained by an institutional third party pursuant to the following authorization:

(i) a court order under 5.2(a)(i) if the record contains highly protected information;

(ii) a court order under 5.2(a)(ii) [5.2(a)(iii) or 5.2(a)(iv)] if the record contains moderately protected information; or

(iii) a subpoena under 5.2(b) if the record contains minimally protected information.

(b) If the record contains highly protected information, a legislature, a court acting in its supervisory capacity, or an administrative agency could consider more demanding restraints for access to the record, such as additional administrative approval, additional disclosure, greater
investigative need, or procedures for avoiding access to irrelevant information.

(c) The protections afforded to privileged information contained in records maintained by institutional third parties and the responsibilities of privilege holders to assert those privileges are those provided by the law applicable in the jurisdiction in which privilege is asserted. The jurisdiction in which law enforcement obtains documents may impose obligations on both institutional third parties to protect what might be privileged information and on law enforcement with respect to the access to, and storage and disclosure of, such information.

To the extent that the NSA obtains this information in the course of its data-collection efforts, a further question arises about the extent to which the NSA should be entitled to access the full content and to share it with other law enforcement agencies without observing otherwise applicable legal process protections. 75 Standard 25-4.2 specifically mentions privilege among the factors that law enforcement should take into account in accessing data, but it is unclear that such niceties are being observed.

V. WHAT DATA SECURITY BREACH LAWS APPLY TO LAWYERS AND LAW FIRMS?

This part of this paper summarizes sources of data breach security law that generally applies to business enterprises, a classification that includes law firms in some cases.

75. See Risen & Poitras, supra note 3, at A 18. The reporters also stated:

The [NSA] is barred from sharing with prosecutors intercepted attorney-client communications involving someone under indictment in the United States, according to previously disclosed N.S.A. rules. But the agency may still use or share the information for intelligence purposes.

... disclosures in recent months from the documents leaked by Mr. Snowden show the agency routinely spies on trade negotiations, communications of economic officials of other countries, and even foreign corporations.

Id. Risen and Poitras also cited the fact that the NSA, following interception of communications of Americans as the DC lawyers may be, is “required to follow so-called minimization rules to protect their privacy, such as deleting the identity of Americans or information that is not deemed necessary to understand or access the foreign intelligence before sharing it with other agencies.”

Id.
A. State Data Security Breach Laws

Lawyers and law firms are subject to a multitude of non-uniform state data security breach laws,76 as well as, depending on the nature of the data, federal laws including HIPPA,77 and other guidance from the federal government, such as the FFEIC Guidance.78

Legislation requiring private entities, or government entities subject to their jurisdiction, to notify individuals of data security breaches that involve breaches of information that includes personally identifiable information, has been enacted by 46 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.79 States with no security breach laws include Alabama, Kentucky, New Mexico, and South Dakota.80

Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data/information brokers, government entities, etc.); definitions of “personal information” (e.g., name combined with SSN, driver’s license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing and method of notice, who must be notified); and exemptions (e.g., for encrypted information).81

Lawyers’ and law firms’ ability to rely on the “safe harbors” for encrypted data that appear in state data security breach laws82 appears to be diminishing proportionately to the new risks that arise as the NSA pursues encryption-breaking capacities.83


80. Id.

81. Id. However, not all States define the term “encryption” and, when defined, the standards are not uniform. See Eric Hibbard, Data Breaches and the Encryption Safe Harbor, at 25, 2012 power point presentation, STORAGE NETWORKING INDUSTRY ASSOCIATION, available at https://www.snia.org/sites/default/education/tutorials/2012/fall/security/EricHibbard_Data-Breach-Encryption-Safe-Harbor_Final.pdf (citing Data Breach Laws: Will They Save or Sink You in a Massive Attack?, RSA Conference 2012, Session: LAW-203 (February 2012)).


B. Federal Trade Commission Section 5 Jurisdiction

In addition, lawyers and law firms are subject to the jurisdiction of the Federal Trade Commission (FTC) and its “unfair and deceptive acts or practices in commerce” jurisdiction under section 5 of the Federal Trade Commission Act.\textsuperscript{84} The FTC has not yet used this jurisdiction against lawyers or law firms that experienced a data security breach. The FTC has used Section 5 against corporations in its jurisdiction that have suffered data security breaches, including its June, 2012 complaint against the collection of affiliates that own and operate Wyndham hotels.\textsuperscript{85} Paragraph 2 of the Complaint summarizes the basis for the FTC’s action:

\begin{quote}
Defendants’ failure to maintain reasonable security allowed intruders to obtain unauthorized access to the computer networks of Wyndham Hotels and Resorts, LLC, and several hotels franchised and managed by Defendants on three separate occasions in less than two years. Defendants’ security failures led to fraudulent charges on consumers’ accounts, more than $10.6 million in fraud loss, and the export of hundreds of thousands of consumers’ payment card account information to a domain registered in Russia. In all three security breaches, hackers accessed sensitive consumer data by compromising Defendants’ Phoenix, Arizona data center.\textsuperscript{86}
\end{quote}

As a result, lawyers and law firms who fail to maintain reasonable security and whose failure “allows” unauthorized persons to gain access to their networks, documents stored in clouds, or long-term archives cause injury to their clients, could be vulnerable to suit by the FTC as well as by their clients.

C. Other Sources of Data Breach Liability for Lawyers and Law Firms

1. The 1995 EU Data Protection Directive

Law firms that operate in the European Union as well as the United States – or who have clients who reside in the European Union’s states – should already be familiar with the 1995 EU Data Protection Directive.\textsuperscript{87} The Directive prohibits transfer of data pertaining to residents unless comparable data protection is afforded by the nation in which the transferee is located.\textsuperscript{88} Disputes

\textsuperscript{86} Id. ¶ 2.
\textsuperscript{88} Id.
prior to the NSA data-gathering disclosures prompted the EU and United States to enter into an agreement providing procedures for enterprises in the United States to comply with the EU’s requirements when they house or import data from the EU. 89

Of fresh, post-Snowden interest to lawyers and law firms operating under the Safe Harbor or with intentions to do business in the EU or represent clients in the EU is the EU justice commissioner’s recent call for bigger fines for breaches of European data security laws. 90

And, lawyers should become aware of, to the extent that they are not already preparing to act on, proposals by Chancellor Angela Merkel of Germany to “create European data networks that would keep emails and other communications on the European side of the Atlantic, farther from prying American eyes…”91

2. Should Lawyers Consider Taking “Commercially Reasonable” Steps to Protect Data from Breaches and What Would Such Steps Entail?

In connection with their responsibilities and responsive strategies they may decide to employ, lawyers and law firms vulnerable to data security breach actions should ask themselves “what is commercially reasonable security?” As explained by one commentator,

As most data breach class actions have been dismissed for lack of damages, courts generally have not examined what might constitute reasonable data security when [private] plaintiffs allege negligence. Although several states have data security laws that require businesses


to adopt reasonable security measures to protect personal information.

These statutes do not define what constitutes reasonable data security. However, in a different context, the First Circuit recently addressed reasonable security under Article 4A of the Uniform Commercial Code. In a case that likely will have wide ranging implications for financial institutions and perhaps other businesses, the court in *Patco Construction Co. v. People’s United Bank* held that a bank failed to provide commercially reasonable security to protect a consumer from fraud. The security procedures proved commercially unreasonable, in part, because the bank posed the same challenge questions for high-risk transactions that it did for ordinary transactions, which was particularly troubling given the prevalence of key-logging malware, about which the bank had been cautioned by its consultants.\(^92\)

The court’s fact-intensive opinion demonstrates that the *crux* of security procedures will be the use – serious or superficial – a bank, or any business, makes of them.\(^93\)

Another commentator made two other highly instructive observations about the First Circuit’s holding in *Patco*.\(^94\) He noted, first, that failure to take action when a security alert triggers a security protocol, not only “may render security procedures ‘commercially unreasonable’ under the U.C.C. Article 4A and, second, that it “may deprive an originator’s bank of the risk allocations and liability limits it sought in its online banking agreement with its customer.”\(^95\)

Translating the sage counsel offered by both of these commentators, lawyers and law firms should be certain that they comply with any cybersecurity policies they establish, they re-evaluate how well they work periodically, and conduct regular training and re-training of all personnel to ensure maximum utility of their policies.

3. Domestic Laws

Other prospective liability may arise under common law negligence, per se negligence, breach of contract, the common law covenant of good faith and fair dealing, and unjust enrichment/restitution.\(^96\)

VI. WHAT RESPONSIBLE STRATEGIES AND STEPS CAN LAWYERS AND LAW FIRMS CONSIDER IN RESPONSE TO THREATSPOSED

---

93. Id.
95. Id. at 190 (footnotes omitted).
The NSA revelations should challenge lawyers’ and law firms to do more to secure the communications they have with and work-product and client-related documents they may have in storage or transmission. The 2012 Amendments to the MRPC raise the stakes for law firms in terms of protecting data and obtaining informed consent. Surveillance activities like the NSA’s also increase the problems that lawyers and law firms have in dealing with risks to data security and in responding to hacking incidents and internal data theft in terms of state- and EU-enacted data security breach notification responsibilities.

Additionally, high-profile data security breaches, such as that experienced by Target in late 2013, demonstrate that breaches can be perpetrated via vulnerabilities that exist in the systems of vendors whose software is allowed to interface with too many internal systems of their customers.

President Obama’s January 17, 2014 Directive on Signals Intelligence does not reduce concerns related to files sent among computers, tablets, and other media that we identified in Red Skies in 2011. Its failure to prohibit future actions such as the NSA-introduced “back-door” vulnerabilities also enhances risks to law firms’ and lawyers’ communications and clients’ data and files. The current state of play in the United States does not relieve lawyers and law firms in the United States from duties they have if they hold data pertaining to residents of the European Union or Canada from storage where it is accessible by the NSA contrary to EU provisions, and it does not absolve them from liability under the data security breach laws of the States or the European Union, described briefly in this article. This is in part because the penetration of firm-applied encryption undercuts lawyers’ and law firms’ ability to qualify for “safe harbors” found in many data security breach notification laws here and abroad. It does nothing to quell concerns that Americans’ communications with clients abroad will be protected by suitable minimization procedures or stopped when the

97. See supra text accompanying notes 26-46.
101. See BAKER & HOSTETLER LLP, supra note 82 (providing information about states that link their data security breach notification “safe harbors” to data encryption). Numerous states limit application of their notification requirements to data that is not encrypted (e.g., Ohio, Arkansas, Delaware, Florida, Georgia, Hawaii, Kansas, Massachusetts). Id. at 15-17.
communications involve sensitive issues that traditional concepts of privilege and confidentiality are implicated.

The stakes are about to become greater for lawyers and law firms. Relatively new demands by clients for their outside law firms to undergo cybersecurity audits adds to the pressures on lawyers and law firms to get their cybersecurity houses in order. In mid-2013, press reports revealed that Bank of America Merrill Lynch was “auditing the cybersecurity policies at its outside law firms, partly under pressure from government regulators.”102 This raises the question, as one commentator put it, “Would Your Firm Pass A Data Security Audit?”103 Target’s experience demonstrates that firms should consider whether their vendors will subject them to security breaches.104

All told, the revelations about the scope of the U.S. government’s surveillance of telecom and other data and its “back door” capabilities, breaches at retailers such as Target, and the heightened responsibilities set forth in the MRPC should cause law firms and solo practitioners to (a) review their current data security policies and facilities and breach notification protocols and (b) re-think where and how files and data related to active projects as well as to archived projects should be managed and stored. The most sensitive data, legally and from the perspective of risks to the firm’s reputation, should be reviewed and stored the most carefully to maintain the greatest degree of protection for the confidential and privileged information it contains.

To evaluate what advice lawyers and law firms already may have about how they may satisfy their duties under the MRPC, described above, to protect clients and their data, I surveyed advice given recently in public forums to lawyers and law firms seeking to fulfill their important data-protection responsibilities. From the plethora of sources of such advice, I identified tasks that lawyers and firms might be encouraged to take to ensure greater protection for their clients’ and the firm’s data as well as some corollaries. The most salient recent pieces of advice encourage lawyers and law firms to:

1. Understand what types of data you hold on clients’ behalf, and the relative risks that each type of data may present.

---


103. See Would Your Firm Pass A Data Security Audit?, LAWBIZ MGMT. (Jul. 11, 2013), http://www.lawbiz.com/coachs_corner_7-11-2013.html (providing a very brief checklist of the major categories of services and storage that lawyers should check on as they evaluate how secure their data and conduct is, including “enterprise security,” “wireless security,” “cloud security,” “email security,” and “insurance coverage.”).

104. See generally supra note 98.
For example, one expert suggests classifying data in terms of three levels of sensitivity and reviewing whether the security procedures are sufficient in light of the differing risks. These classes include: “public” information that is accessible to the public and that poses little risk to the firm’s reputation, including information on the firm’s public website; “sensitive or confidential” information that could have a moderately adverse effect on the firm’s reputation such as data covered by non-disclosure agreements, competitive market research, and the like; and “restricted” information that poses the highest risks to reputation including HIPPA data, non-public personal information about clients, employees and clients’ counter-parties, or the formula for Coca Cola.

But even more importantly, to understand where information relative to operational issues (how many people need to staff a project in a company) and

2. Decide where the highest-value data should be stored and how access to it will be protected. One basis for choosing private clouds, as opposed to public clouds, for high-sensitivity data is that if a government agency or other person wants access to it via a form of legal process, at least the firm knows about it.

3. Identify the cloud computing adoptions across the office or firm and the identity and the terms on which each cloud provider is operating with your office or firm.

4. Determine which providers are involved in public and private clouds in use or that have been used. Read the contracts with each provider and any amendments to them since original execution.

106. See id.
107. See id.
108. See id.
5. Raise all employees’ understanding of the importance of strong data security habits. One commentator suggests specific annual training programs, as well as other steps such as requiring different passwords for different sites or applications, restricting software downloads to trusted sites, verifying installation of anti-virus software and firewalls, and locking computers before leaving them (even for short periods) and not storing sensitive data on removable media.\footnote{112}

6. Consider the affect on representation of clients if the storage services your firm uses, whether internal, outsourced, or in the cloud, became unavailable or was compromised.\footnote{113}

7. Create a master protocol that addresses various aspects of data management and security, including non-technical legal requirements for privacy rights, non-U.S. and out-of-state data security standards and breach notifications, and the like. This could include the firm’s business continuity plan, disaster recovery plan, incident response plan, physical security plan, and bring-your-own-device/bring-your-own-network policies.\footnote{114}

8. Be prepared for requests by clients for the firm to undergo an information security audit.\footnote{115}

9. Consider the greater risks of having computing devices on higher floors of buildings because the computer’s emanations become easier to intercept.\footnote{116}

10. Expect data security vigilance from everyone in the firm and take prompt corrective action including re-training or sanctions against those who do not meet protocols or expectations.\footnote{117}

\footnote{111. See Trope & Hughes, supra note 4, at 185-198 (discussing different cloud providers’ contracts and their amendments to 2011).}
\footnote{112. See id.}
\footnote{113. Id. See also Five Things, supra note 105. Ms. Deuschle also recommends asking about the certifications that the cloud service provider you use or plan to use may have – viz., SOC 1, SOC 2, or SOC 3, ISO 27001, NIST 800-53, and CSA’s Security, Trust & Assurance Registry (known as STAR) as well as asking whether the provider performs regular “penetration tests” using independent firms to identify risks in the application so that remedies can be devised before the breach can occur. See id.}
\footnote{114. See Nelson & Simek, supra note 102.}
\footnote{116. See Trope & Hughes, supra note 4, at 148 (citing Michael A. Caloyannides, Forensics is so “Yesterday”, IEEE SECURITY & PRIVACY, Mar.-Apr. 2009, at 21).}
\footnote{117. See Five Things, supra note 105.}
11. Consider, if the client base includes clients not domiciled in the United States, the additional ethical requirements placed on lawyers and firms operating where those clients are based, and the likelihood that clients – or their governments – will demand that data related to their interests and persons be stored where it can enjoy the highest degree of protection from U.S. government surveillance.

12. Create and maintain a diagram showing where the firm’s data is stored.\textsuperscript{118}

13. Never let control of your digital assets out of your sight.\textsuperscript{119}

14. Never give an order for security that you cannot obtain or you know will be disobeyed.\textsuperscript{120} Users seek short cuts. Law firms are not likely to be different.

15. Law firms and lawyers should not bring any client data on laptops to meetings abroad and do not seek to receive client data while they are abroad, particularly if the travel involves certain nations more inclined to search electronics at their borders, such as the United States and China. Care also occasionally mandates routing of travelers who have knowledge of significant high-value details away from certain nations if they are traveling with or have substantive personal knowledge of trade secrets and the like.\textsuperscript{121}

16. Do not assume that encryption is as much in use as you might use it.\textsuperscript{122}

And,

17. Whatever else lawyers or law firms may do to protect their clients, never take clients’ privileged or confidential data from the office on a laptop and then leave the laptop unattended.\textsuperscript{123}

However helpful the items on the list above may seem, the big question remains whether what lawyers and law firms do will satisfy lawyers or their clients that clients’ documents and data stored in the cloud are safe from unexpected or excessive government access or from other unauthorized access.

\textsuperscript{118} See Nelson & Simek, supra note 102.

\textsuperscript{119} Cormac Herley, More is Not the Answer, SECURITY & PRIVACY, IEEE, Jan.-Feb. 2014, at 16.

\textsuperscript{120} Id.

\textsuperscript{121} Conversation with Roland L. Trope, February 2, 2014.

\textsuperscript{122} See Nelson & Simek, supra note 102.

\textsuperscript{123} Susan Gainen, 6 Rules for Protecting Confidential Information, LAWYERIST (May 8, 2010), http://lawyerist.com/rules-for-protecting-confidential-information/.
Also, clients are likely to express concerns about whether their competitors, counter-parties and opponents will find it possible to access data stored in the cloud – despite justifiable claims of privilege or confidentiality – merely because these data have been placed in the hands of third parties who may consent, perhaps limited by contracts and perhaps not, to divulge the data stored with them.

VII. SOME LUDDITE-LEANING CONCLUSIONS

Recent events including the NSA data-mining programs, including the DC law firm-Government of Indonesia incident described above, and the late 2013 Target and Neiman Marcus data security breaches compel the conclusion that lawyers and law firms should rethink their uses of cloud computing generally, as well as the manner in which they protect all files, documents, and communications with clients, and to select means to store the most sensitive data and all privileged data somewhere that still enjoys more protection from government access and surveillance than data stored in the cloud. This is true, even as described above, the privilege can only be waived by the client – and not by government interception – for the purposes of criminal prosecutions.

These events strongly suggest that, for the most sensitive files and data, lawyers and law firms should revert to old-fashioned methods to protect client communications and safeguard clients’ property, including confidential and other files. Such old-fashioned methods include using manual typewriters, attending meetings in person as opposed to via teleconferences, Skype or telephone calls, and locking paper and electronic records in file cabinets in lawyers’ offices and storing sensitive archives in actual warehouses (where the thief would need a good map or lots of time to find the high-value records they can access electronically otherwise). These physical and administrative security measures – in addition to appropriate technical security measures – will allow lawyers and law firms to control access to sensitive information in more effective, if less technology dependent ways. It also means that in the trio of possible means of securing data – physical, administrative and technical safeguards – that physical and administrative safeguards are no less important, and possibly more important and easy to enforce than the technical safeguards on which we have placed so much emphasis recently.

Enhanced security for communications with clients and for data stored also means renewing restrictions on the use of smart phones and tablets, laptops and off-site desktops, flash drives and other peripherals. These restrictions for confidential and privileged data and communications also include not using

---

124. See Kremlin Security Agency to buy typewriters “to avoid leaks”, BBC (Jul. 11, 2013), http://www.bbc.co.uk/news/world-europe-23282308 (explaining that the Kremlin Security Agency’s decision to use typewriters is attributed to Edward Snowden’s leaks of NSA policies and data and the unique “handwriting” that enables documents to be associated with each machine).
voicemail or similar systems that involve telecomm that the NSA, other governments or the client’s competitors might be able to obtain. Does it make me sound like a Luddite? I imagine that it will to many readers – particularly proponents of the technology-solves-all approaches to efficiency and productivity issues.

Revelations about data mining by the NSA and the U.K.’s spy agencies also necessitates more robust conversations with clients about the sensitivity of their files and records and of their communications with lawyers. This means staying abreast of developments and sharing findings with clients, and involving them in the cost-benefit analyses of how and where to store files and records, and how to conduct necessary communications. The 2012 additions to MRPC Rule 1.6(c)’s comments also require consideration of steps the lawyer needs to be conscious of and prepared for in terms of compliance with state or federal data security breach laws so that they can obtain informed consent from their clients.125

There is no question that the NSA’s metadata-collection program, as well as the published reports that the NSA can reach certain content elements as well as metadata in messages,126 will make it much harder for lawyers and law firms to protect the confidentiality and privilege of their client’s communications with them and other sensitive data from the government. Commentators have predicted that the “back doors” that the NSA has introduced also threaten to facilitate unauthorized access by hackers, and possibly by competitors.127

The NSA surveillance of telecomm and its introduction of radio-frequency-enabled “back doors” to many computing and telecomm devices chips away at the reasonable expectation of privacy in communications and document exchanges between lawyers and their clients that have provided the framework for access by government agencies to tangible records in the hands of third parties and for other purposes in “search and seizure” jurisprudence since United States v. Katz128 and United States v. Miller.129 In connection with MRPC Rule 1.6,130 this recent knowledge alters otherwise applicable protections for documents, files and communications under domestic law and, at least equally

125. See supra text accompanying notes 53-57.
128. 389 U.S. 347 (1967) (holding that warrantless wiretapping of public pay phones to obtain defendant’s conversations violates reasonable search and seizure protections of the Fourth Amendment).
129. 425 U.S. 435 (1976) (holding that defendant had no expectation of privacy, and hence no Fourth Amendment protections, in records held by two banks with which he dealt for which subpoenas had been issued, and no right to suppression of evidence obtained).
130. MODEL RULES OF PROF’L CONDUCT R. 1.6(c) cmt. 17 (2012).
important, it alters or jettisons terms of otherwise applicable confidentiality agreements – among the factors cited in Comment 17 to be considered in determining the reasonableness of the lawyer’s normal precautions. After all, as one commentator observed: “Because … [cybersecurity] standards [such as ISO 27001] are not compulsory … your protection in court against legal redress always boils down to due diligence.”

To make that point even more relevant to lawyers and law firms, just as I was completing the draft of this paper for this symposium, the National Institute of Standards and Technology (“NIST”) issued its newest standards, the Framework for Improving Critical Infrastructure Cybersecurity. The Executive Summary summarizes reasons why diligent management of cybersecurity risk is important: “Similar to financial and reputational risk, cybersecurity risk affects a company’s bottom line. It can drive up costs and impact revenue. It can harm an organization’s ability to innovate and to gain and maintain customers.”

So, after looking at the issues raised by lawyers’ professional responsibilities in the post-Snowden era, my mind keeps spinning through Joni Mitchell’s famous, pre-Internet and pre-cell phone – and definitely pre-cloud computing and storage – refrain:

I’ve looked at clouds from both sides now,
From up and down, and still somehow
it’s cloud illusions I recall,
I really don’t know clouds at all.

Responsible steps that lawyers and law firms can take include all of the individual cyber-smart steps mentioning in Part VI of this paper and the additional steps mentioned by Nelson & Simek. They also include old-fashioned, low-tech physical and administrative steps such as mentioned above. And some of these low-tech steps are as old-fashioned as meeting in person to discuss ultra-sensitive issues, using manual typewriters, and locked filing cabinets or vaults to store clients’ trade secrets, medical information, non-public personally identifiable information, and negotiations over mergers and acquisitions or the like. Some of the responsible storage and communications of clients’ records and data security practices really might not include clouds at all – even if it makes me unpopular with cloud computing vendors.

131. Id.
134. Id. at 1.
137. See supra, pp. 22-23.
FEDERAL CYBER-SECURITY LAW AND POLICY: 
THE ROLE OF THE FEDERAL ENERGY 
REGULATORY COMMISSION 

A PAPER PREPARED FOR THE 2014 LAW + INFORMATICS SYMPOSIUM 
ON CYBER DEFENSE STRATEGIES AND RESPONSIBILITIES FOR INDUSTRY

Susan J. Court∗

I. INTRODUCTION

The Federal Energy Regulatory Commission (“FERC” or “Commission”) is the only Federal agency that sets standards governing cyber-security for the electric utility industry, including investor-owned and publicly owned utilities, and enforces those standards by fining entities, even other Federal agencies that violate them. Other Federal agencies can address and even penalize companies and individuals for breaches of cyber-security rules, directives, or protocols; but none of them specifies upfront, the way FERC does, how to protect against a cyber-security event on the nation’s electric grid. Accordingly, this paper will examine the role that the Commission plays in the Federal government’s involvement in cyber-security law and policy. It will first review the background to the Commission’s responsibility, then discuss relevant FERC rules and policies, and conclude with an overview of the agency’s efforts to enforce those rules as well as the policies and the prospect for an expansion of the Commission’s authority.

II. BACKGROUND

FERC regulates important aspects of interstate energy transactions and administers, *inter alia*, the Interstate Commerce Act (with respect to interstate oil pipeline transportation); the Federal Power Act (with respect to the interstate transmission and wholesale sales of electric energy, and the construction of hydroelectric projects); and the Natural Gas Act and the Natural Gas Policy Act (with respect to the interstate transportation and wholesale sales of natural gas and the construction of natural gas and liquefied natural gas facilities).1 Traditionally, until 2005, the Commission primarily regulated investor-owned companies that provide service to other companies. In 2005, Congress greatly expanded the Commission’s authority by enacting the Energy Policy Act

---


As relevant here, EPAct directed FERC to establish a program to ensure the reliability of the U.S. “Bulk-Power System” (i.e., the nation’s electric grid) by setting standards to apply to the users, owners, and operators of that system. This direction increased the number of entities subject to FERC’s Federal Power Act electric jurisdiction from approximately 200 investor-owned electric utilities to over 1,500 organizations, including municipal utilities, Federal power administrations, electric cooperatives, and even the Tennessee Valley Authority and the U.S. Army Corps of Engineers. EPAct also made violations of those standards subject to hefty penalties that could be as high as $1 million a day for the duration of the violations, thereby making FERC an enforcement agency as well as an economic regulator.

The impetus for EPAct’s reliability provisions was the massive blackout of the North American electric grid that occurred in August 2003. At the time, it was the second largest blackout in history, affecting an estimated fifty million people. A subsequently prepared report issued jointly by the United States and Canada described the blackout and its impact as follows:

On August 14, 2003, large portions of the Midwest and Northeast United States and Ontario, Canada, experienced an electric power blackout. The outage affected an area with an estimated 50 million people and 61,800 megawatts (MW) of electric load in the states of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, New Jersey, and the Canadian province of Ontario. The blackout began a few minutes after 4:00 pm Eastern Daylight Time (16:00 EDT), and power was not restored for 4 days in some parts of the United States. Parts of Ontario suffered rolling blackouts for more than a week before full power was restored. Estimates of total costs in the United States range between $4 billion and $10 billion (U.S. dollars). In Canada, gross domestic product was down 0.7% in August.

---

7. Previously, in 1999, Brazil experienced a larger blackout, affecting an estimated 97 million people. Since 2003, there have been larger blackouts but not in the United States. Brazil and Paraguay experienced a blackout in 2009, affecting 87 million; Java and Bali experienced a blackout in 2005, affecting 100 million people; and India experienced a blackout in 2012, affecting 670 million people. Most Powerful Blackouts In History, CLEAN TECHNICA, (Nov. 27, 2012), http://cleantechnica.com/2012/11/26/most-powerful-blackouts-in-history/.
there was a net loss of 18.9 million work hours, and manufacturing shipments in Ontario were down $2.3 billion (Canadian dollars). 8

The extent of the blackout, hours after it began, can be seen on this satellite picture:

The Blackout Report also analyzed in great detail the causes of the blackout and made many recommendations. 9 In general, the report found:

The Ohio phase of the August 14, 2003, blackout was caused by deficiencies in specific practices, equipment, and human decisions by various organizations that affected conditions and outcomes—for example, insufficient reactive power was an issue in the blackout, but it was not a cause in itself. Rather, deficiencies in corporate policies, lack of adherence to industry policies, and inadequate management of reactive power and voltage caused the blackout, rather than the lack of reactive power. 10

9. Id. at id.
10. Id. at 18. By way of background:

A generator typically produces some mixture of “real” and “reactive” power, and the balance between them can be adjusted at short notice to meet changing
While the origin of the blackout is commonly thought to have been a tree touching a power line of a Cleveland utility (“First Energy”), the report identified several specific causes, including the First Energy’s failure to assess and understand the inadequacies of its system, operate its system with appropriate voltage criteria, recognize or understand the deteriorating condition of its system, and manage adequately tree growth in its transmission rights-of-way; as well as the failure of the interconnected grid’s reliability organizations to provide effective real-time diagnostic support.11

The Blackout Report also specifically criticized the existing voluntary organization of electric utilities that oversaw the reliability of the electric grid not because it was “an inadequate or ineffective organization, but rather because it ha[d] no structural independence from the industry it represent[ed] and ha[d] no authority to develop strong reliability standards and to enforce compliance with those standards.”12 Accordingly, the report strongly recommended that Federal legislation be enacted to make that happen.13

Congress agreed with the Blackout Report and, less than two years later, enacted EPAct, which, _inter alia_, added a new section 215 to the Federal Power Act (“FPA”) to provide for a system of mandatory, enforceable Reliability Standards.14 Briefly, FPA section 215 required the Commission to certify a single Electric Reliability Organization (“ERO”) to oversee the reliability of the United States’ portion of the interconnected North American Bulk-Power System, subject to Commission oversight, and authorized the Commission to approve all ERO actions and, as appropriate, to independently enforce the Reliability Standards.15 FPA section 215 provided that the ERO would be

---

11. _Id._ at 18.
12. _Id._ at 21.
13. _Id._
15. _Id._ at § 824(c). FPA section 215 describes the “bulk-power system” as including “the facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof), and electric energy from generation facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy.” _Id._ at § 824(o)(a)(1). FERC uses the term “bulk electric system” (“BES”) for the applicability of the standards, and defines the term generally as the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission sources are generally not included in this definition. See Revisions to Electric Reliability Organization Definition of Bulk Electric System and Rules of Procedure, 144 FERC 61174 (2013). On June 6, 2013, the Commission extended the effective date conditions. Real power, measured in watts, is the form of electricity that powers equipment. Reactive power, a characteristic of AC systems, is measured in volt-amperes reactive (VAR), and is the energy supplied to create or be stored in electric or magnetic fields in and around electrical equipment. Reactive power is particularly important for equipment that relies on magnetic fields for the production of induced electric currents (e.g., motors, transformers, pumps, and air conditioning.) Transmission lines both consume and produce reactive power. _Id._ at 8.
responsible for developing and enforcing the mandatory Reliability Standards that would apply to all users, owners and operators of the Bulk-Power System, and submit each proposed Reliability Standard to the Commission for approval. The ERO was permitted to delegate its enforcement responsibilities to Regional Entities, subject to the Commission’s approval. The ERO or the Regional Entities would then be responsible for monitoring compliance with the Reliability Standards; could direct a user, owner or operator of the Bulk-Power System that violates Reliability Standard to comply with the Reliability Standard; and impose a penalty on a user, owner or operator for violating a Reliability Standard, subject to review by, and appeal to, the Commission.

In the years following the enactment of EPAct, the Commission issued a series of orders that implemented FPA section 215. Four orders issued in 2006 and 2007, in particular, established the Federal, mandatory reliability program for the nation’s electric grid.

- On February 3, 2006, the Commission issued Order No. 672, which promulgated regulations, codified in Part 39 of Title 18 of the Code of Federal Regulations, that established the criteria that an entity must satisfy to qualify to be the ERO, procedures under which the ERO may propose new or modified Reliability Standards for Commission review, principles pertaining to the funding of the ERO, procedures governing an enforcement action by the ERO, a Regional Entity, or the Commission, and criteria under which the ERO may enter into an agreement to delegate authority to a Regional Entity for the purpose of proposing Reliability Standards to the ERO and enforcing those standards.16

- On July 20, 2006, the Commission issued an order that certified the North American Electric Reliability Corporation (“NERC”) as the ERO.17

- On March 16, 2007, the Commission issued Order No. 693, in which it approved 83 of 107 proposed Reliability Standards developed by NERC, to become effective June 18, 2007.18 Order No. 693 also added a new Part 40 to the Commission’s regulations, 18 C.F.R. Part 40, which stated that the standards applied to all users, owners, and operators of the Bulk-Power System within the

---


United States (other than Alaska and Hawaii) and required that each Reliability Standard identify the subset of users, owners, and operators to which that particular Reliability Standard applies. The new regulations also required that each Reliability Standard approved by the Commission would be maintained on the ERO’s Internet website.

- On April 19, 2007, the Commission issued an order accepting the ERO’s agreements with eight Regional Entities and approving those entities' 2007 business plans. As depicted below, the eight Regional Entities are Florida Reliability Coordination Council, Midwest Reliability Organization, Northeast Power Coordinating Council, ReliabilityFirst Corporation, SERC Reliability Corporation, Southwest Power Pool, RE, Texas Reliability Entity, and Western Electricity Coordinating Council.

The April 19 order also approved a Compliance Monitoring and Enforcement Program, which set out the structure and processes to be used by the Regional Entities to enforce the mandatory Reliability Standards.

By way of further background, Order No. 693 identified fourteen categories of Mandatory Reliability Standards, including cyber-security standards referred

---

20. Id. at 61261.

The standards apply to the users, owners, and operators of the Bulk-Power System, who are registered by NERC according to the function they perform within that system (and hence are called “Registered Entities”). Those functions include: Balancing Authority, Distribution Provider, Generator Owner, Generator Operator, Interchange Authority, Load Serving Entity, Planning Authority, Purchasing Selling Entity, Reliability Coordinator, Resource Planner, Reserve Sharing Group, Transmission Owner, Transmission Operator, Transmission Planner, and Transmission Service Provider.

Since the enactment of EPAct, the Commission has approved over 100 mandatory Reliability Standards, which in turn include over 1,000 separate requirements, and NERC has registered 1,646 users, owners, and operators for a total of 4,782 functions.

III. CRITICAL INFRASTRUCTURE PROTECTION ("CIP") STANDARDS

To date, the Commission has approved eleven CIP mandatory Reliability Standards; however, there have been several versions of these standards in effect since April 2007. Currently, the third version is the law and will be replaced by the fifth version to be effective in April 2016. The Commission approved the first CIP standard—CIP-001-1 (Sabotage Reporting)—in Order No. 693. As explained there:

21. Mandatory Reliability Standards For the Bulk-Power System, 72 Fed. Reg. 16416-01, 16463 (Apr. 4, 2007). As defined by NERC for the purposes of the CIP standards, critical infrastructure includes facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.

22. See generally id.


The goal of [this standard] is to ensure that operating entities recognize sabotage events and inform appropriate authorities and each other to properly respond to the sabotage to minimize the impact on the Bulk-Power System. The Reliability Standard requires that each reliability coordinator, balancing authority, transmission operator, generation operator and load serving entity have procedure for recognizing and for making operating personnel aware of sabotage events, and communicating information concerning sabotage events to appropriate “parties” in the Interconnect.26

CIP-001-1 became effective on June 4, 2007.27 Nine months later, on January 18, 2008, the Commission approved eight additional CIP standards in Order No. 706.28 Subsequently, the Commission approved Version 2 and Version 3 (“CIP V3”) of these standards, which became effective on April 1, 2010 and October 1, 2010, respectively.29 The Commission also approved a fourth version, on April 19, 2012, in Order No. 761, but delayed the effectiveness of this version until October 1, 2014,30 a time by which Version 5 (“CIP V5”) (discussed in greater detail below) would most likely make compliance with Version 4 unnecessary.31 In fact, in the order in which the Commission approved CIP V5, the Commission expressly rescinded the fourth version of the CIP standards.32

In all versions of the CIP standards, the threshold issue is what assets are subject to the requirements. This issue is addressed primarily in CIP-002, which deals with the identification of critical cyber assets.33 For the purpose of CIP V3, which is the law until April 2016, the analysis involves the definitions of four terms, the first of which is statutory: (1) “reliable operation,” which means “operating the elements of the Bulk-Power System within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation or cascading failures of such system will not occur as a result of a sudden disturbance, including a cyber-security incident, or unanticipated failure

27. Id. at 16598.
of system elements”; 34 (2) “critical assets,” which are “facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System”; (3) “cyber assets,” which are “programmable electronic devices and communication networks including hardware, software, and data”; and finally (4) “critical cyber assets,” which are “cyber assets essential to the reliable operation of critical assets.” 35 Accordingly, as the Commission has consistently held, the accurate identification of critical assets and critical cyber assets is the cornerstone of the CIP Reliability Standards, because “it acts as a filter, determining whether a responsible entity must comply with the remaining CIP requirements in CIP-003-1 through CIP-009-1.” 36

Against this backdrop, the eight CIP Reliability Standards approved in Order No. 706 are: 37

- **CIP-002-1–Cyber Security–Critical Cyber Asset Identification**, which requires a responsible entity to identify its critical assets and critical cyber assets using a risk-based assessment methodology. 38

- **CIP-003-1–Cyber Security–Security Management Controls**, which requires a responsible entity to develop and implement security management controls to protect critical cyber assets identified in CIP-002-1.

- **CIP-004-1–Cyber Security–Personnel and Training**, which requires personnel with access to critical cyber assets to have identity verification, a criminal check, and employee training.

- **CIP-005-1–Cyber Security–Electronic Security Perimeters**, which requires the identification and protection of an electronic security perimeter and access points, where the perimeter is to encompass the critical cyber assets identified by the methodology required in CIP-002-1.

- **CIP-006-1–Cyber Security–Physical Security of Critical Cyber Assets**, which requires a responsible entity to create and maintain a physical security...

---

37. Id. at 61203.
38. A “responsible entity” is a Registered Entity subject to the CIP mandatory standards. Not all Registered Entities are responsible entities as not all Registered Entities are subject to the CIP mandatory standards. See Compliance & Enforcement, N. Am. Elec. Reliability Corp., http://www.nerc.com/pa/comp/Pages/Default.aspx (last visited May 22, 2014).
plan that ensures that all cyber assets within an electronic security perimeter are kept in an identified physical security perimeter.

- **CIP-007-1–Cyber Security–Systems Security Management**, which requires a responsible entity to define methods, processes, and procedures for securing the systems identified as critical cyber assets, as well as the non-critical cyber assets within an electronic security perimeter.

- **CIP-008-1–Cyber Security–Incident Reporting and Response Planning**, which requires a responsible entity to identify, classify, respond to, and report cyber security incidents related to critical cyber assets.

- **CIP-009-1–Cyber Security–Recovery Plans for Critical Cyber Assets**, which requires the establishment of recovery plans for critical cyber assets using established business continuity and disaster recovery techniques and practices.

NERC described these standards as providing:

> a comprehensive set of requirements to protect the Bulk-Power System from malicious cyber-attacks. They require Bulk-Power users, owners, and operators to establish a risk-based vulnerability assessment methodology to identify and prioritize critical asset and critical cyber assets. Once the critical cyber assets are identified, the CIP Reliability Standards require, among other things, that the responsible parties establish plans, protocols, and controls to safeguard physical and electronic access, to train personnel on security matters, to report security incidents, and to be prepared for recovery actions.[39]

FERC also approved NERC’s implementation plan that provided for a three-year phase-in to achieve full compliance with all of the requirements in order to give responsible entities enough time to purchase and install new cyber software and equipment and develop new programs and procedures to achieve compliance.[40] Furthermore, recognizing the challenges presented by the new CIP standards, the Commission allowed responsible entities to seek exceptions from coverage of those standards, especially with respect to long-life equipment in place that is not readily compatible with a modern environment where cyber security issues are a concern.[41]


40. Id. at 61214.

As noted, the next version of the mandatory CIP Reliability Standards—CIP V5—is on the horizon. On November 22, 2013, the Commission approved a final rule—Order No. 791—that modified CIP-002-3 through CIP-009-3 and added two new standards, CIP-010-1 and CIP-011-1. Generally, the Commission agreed with NERC’s proposal, finding that it represented an improvement over the currently effective standards because it includes new cyber security controls and extends the scope of the systems that are protected by the standards.

Briefly, the CIP V5 standards to be effective in April 2016 are:

- **CIP-002-5--Cyber Security–BES Cyber System Categorization** redefines a BES Cyber Asset that “if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System,” and defines a BES Cyber System as “one or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.” This standard also requires a Registered Entity to classify its facilities into three categories of BES Cyber Systems. High Impact covers large Control Centers, Medium Impact covers generation and transmission facilities, and Low Impact covers all other BES Cyber Systems. Importantly, once a responsible entity identifies a BES Cyber System under CIP-002-5, it would be required to comply with the controls included in the remaining standards.

- **CIP-003-5--Cyber Security–Security Management Controls** requires approval by a CIP Senior Manager of the documented cyber security policies related to the remaining standards. It also requires implementation of policies related to cyber security awareness, physical security controls, electronic access controls, and incident response to a Cyber Security Incident for those assets that have Low Impact BES Cyber Systems under CIP-002-5 categorization process.

- **CIP-004-5--Cyber Security–Personnel and Training** requires documented processes or programs for security awareness, cyber security training, personnel risk assessment, and access management. Specific requirements include training for visitor control programs, electronic interconnectivity supporting the

43. _See_ Id.
44. _Id._
45. _Id._ at ¶ 19-33.
46. _Id._ at ¶ 21.
operation and control of BES Cyber Systems, storage media as part of the treatment of BES Cyber Systems Information, and a seven year criminal history check covering all locations where the individual has resided for six consecutive months.

- **CIP-005-5–Cyber Security–Electronic Security Perimeters** focuses on the discrete Electronic Access Points rather than the logical “perimeter,” which is the focus of the currently effective standard.

- **CIP-006-5–Cyber Security–Physical Security of BES Cyber Systems** is intended to manage physical access to BES Cyber Systems by specifying a physical security plan to protect BES Cyber Systems against compromise that could lead to misoperation or instability.

- **CIP-007-5–Cyber Security–Systems Security Management** addresses system security by specifying technical operations, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability of the bulk electric system. For example, among other things, the responsible entity will be required to document how it addresses the malware risk for each BES Cyber System, but not be required to prescribe a particular technical method in order to account for potential technological advancement.

- **CIP-008-5–Cyber Security–Incident Reporting and Response Planning** mitigates the risk to the reliability operation of the bulk electric system resulting from a Cyber Security Incident by specifying incident response requirements. For example, responsible entities will be required to report Cyber Security Incidents within one hour of recognition, to verify response plan effectiveness and consistent application in responding to a Cyber Security Incident, and provide for an after-action review for tests or actual incidents, and an update to the Cyber Security Incident response plan based on those lessons learned.

- **CIP-009-5–Cyber Security–Recovery Plans for BES Cyber Systems** provides for the recovery of the reliability functions performed by BES Cyber Systems by specifying a recovery plan to support the continued stability, operability, and reliability of the bulk electric system. For example, a responsible entity must have controls to protect data that would be useful in the investigation of an event that results in the execution of a Cyber System recovery plan.

- **CIP-010-1–Cyber Security–Configuration Change Management and Vulnerability Assessments** specifies configuration change management requirements to detect unauthorized modifications to BES Cyber Systems and to
ensure proper implementation of cyber security controls while promoting continuous improvement of a responsible entity’s cyber security posture.

- **CIP-011-1–Cyber Security–Information Protection** specifies information protection controls to prevent unauthorized access to BES Cyber System Information and reuse and disposal provisions to prevent unauthorized dissemination of protected information.

While the Commission generally approved the CIP V5 standards as proposed by NERC, the Commission also directed NERC to provide more information on certain requirements to support their continued inclusion in the standards. For example, even though the Commission approved the revised definition of BES Cyber Asset in CIP-002-5, it directed NERC to conduct a survey of Cyber Assets that are included or excluded under the new BES Cyber Asset definition during the implementation periods, to gain a better understanding of the BES Cyber Asset definition.47 Based on that data, FERC told NERC to explain in an informational filing: (1) specific ways in which entities determine which Cyber Assets meet the 15 minute parameter; (2) types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from each region participating in the implementation study on lessons learned with the application of BES Cyber Asset definition.48

Finally, with respect to the CIP V5, NERC, the Regional Entities, and the responsible entities have been engaged since early 2013 in efforts to transition to the new standards. Each group has dedicated staff to meet three objectives through outreach and training:

- To improve industry understanding of the technical security challenges that must be addressed in order to comply with CIP V5 standards, especially understanding the material differences between Version 3 and Version 5;

- To ensure that industry understands what will be expected of its members to comply with the new standards, including what evidence they must retain to demonstrate compliance; and

- To understand what technical and compliance related resources and efforts are needed to transition and manage compliance with CIP V5 standards.49

---

47. *Id.* at ¶ 124.
49. N. AM. ELEC. RELIABILITY CORP., AGENDA COMPLIANCE COMMITTEE MEETING (Nov. 6, 2013).
IV. ENFORCEMENT OF MANDATORY CIP RELIABILITY STANDARDS

As mentioned earlier, the Regional Entities use the framework called the Compliance Monitoring and Enforcement Program, approved by the Commission in 2007, to ensure compliance by the Registered Entities with the mandatory Reliability Standards.\(^{50}\) They use numerous tools to that end, including conducting audits and spot checks, reviewing self-certifications (of compliance) and self-reports, and pursuing complaints and investigations of alleged violations. Since the standards first became effective in June 2007, the ERO Enterprise has processed thousands of violations and collected millions of dollars in fines.\(^{51}\) As relevant here, since they became effective, the CIP Reliability Standards have consistently accounted for the majority of the violations processed by the Regional Entities, and submitted to the Commission through NERC. For example, in the third quarter of 2013, the top ten violated standards, which closely followed the trend for the previous four quarters, were CIP-007, CIP-006, CIP-005, PRC-005, CIP-004, CIP-002, CIP-003, VAR-002, CIP-009, and FAC-009.\(^{52}\)

There are two reasons in particular for the high incidence of CIP violations. The CIP standards—indeed, even the concept of CIP standards—are relatively new. While many of the other standards were in place, albeit on a voluntary basis, for many years before the enactment of EPAct in 2005, the CIP standards were only developed in the past few years as the technology became more sophisticated and the need to secure cyber assets became more apparent. As a consequence, the responsible entities have less experience in complying with the CIP standards than they have with the other standards. Also, NERC and the Regional Entities have focused their compliance and enforcement resources and efforts on the CIP standards as they became more aware of the critical need for heightened cyber security. To this end, for example, the Regional Entities have increased their staffs and made a concerted effort to hire auditors and enforcement personnel with relevant technical experience.\(^{53}\)

---

52. See N. Am. Elect. Reliability Corp., Agenda Compliance Committee Meeting (Nov. 6, 2013).
53. Most of the Regional Entities also participated in the NERC Grid Security Exercises (“GridEx”), on November 16-17, 2011, and November 13-14, 2013. GridEx is a biennial international grid security exercise that uses best practices from the Department of Homeland Security, the Federal Emergency Management Agency, and the National Institute of Standards and Technology. The 2011 GridEx exercise, for example, was designed to validate the readiness of the Electricity Sub-sector to respond to a cyber-security incident, strengthen Registered Entities’ crisis response functions, and provide input for internal security program improvements. Overall, the exercise was widely regarded across industry and government as a critical imperative in preparing
Once a Regional Entity has confirmed a violation of a standard, and, assuming the Registered Entity does not object to or settles with the Regional Entity on a remedy, the Regional Entity submits the case to NERC’s Board of Trustees. If the Board agrees with the Region’s resolution of the matter, the NERC staff submits the case to the FERC in a filing called a Notice of Penalty (“NOP”). FERC assigns the case a docket number, starting with the letters “NP.” The notice becomes final after thirty days, unless the Commission “tolls” the time for acting on the matter. With few exceptions, the Commission has allowed NERC’s NOPs, including those involving CIP violations, to become effective by operation of law, i.e., by not taking further action on the submission, since the original thirty-seven NOPs were filed in June 2008. As a consequence, there is very little FERC action that would be considered “FERC case law,” and there is no court decision on the enforcement of the Reliability Standards. For members of the electric utility industry and the public in general, the only insight into what constitutes a violation, at least in the view of the Regional Entities, is found in the records that NERC submits to the FERC in the NOP filings.

Illustratively, on October 31, 2012, NERC filed an NOP, in Docket No. NP13-1-000, which included a settlement between the Western Electric Coordinating Council (“WECC”) and an Unidentified Registered Entity (“URE”) resolving WECC’s determination and findings of the violations of CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP-006, and CIP-007. The URE agreed to the assessed penalty of $200,000. With respect to CIP-002-1, WECC pointed out that the URE had self-reported that during an internal review of compliance with the CIP Standards, and in connection with the commencement of its annual review of Critical Cyber Assets (“CCA”), the URE discovered that it failed to
identify 13 CAAs essential to the operation of its Critical Assets (CAs). The URE had two managers who were responsible for identifying CCA, and also relied on electronic records to identify CCAs and develop lists. However, during its annual review process, the URE discovered its lists of CCAs were insufficient. With respect to the violation of CIP-003-1, the URE self-certified that it was not in compliance. Even though the URE had established and documented a process for change control, the process failed to effectively control changes made to its CCA hardware or software, and the URE lacked a process that explicitly governed managing configuration changes.

On February 28, 2013, NERC filed an NOP, in Docket No. NP13-24-000, which included a settlement between WECC and three URE’s arising out of WECC’s determination and findings of violations of CIP-006-1, CIP-004-3, CIP-006-1, and CIP-007-2. The URE’s agreed to an assessed penalty of $151,500. With respect to CIP-006-1, WECC explained that the URE self-reported that it had failed to provide alarming for five card readers that controlled access to three Physical Security Perimeters (“PSPs”). Four of the card readers controlled access to the blackstart human machine interface (“HIMI”) PSP at two of the URE’s facilities. The card readers involved were incorrectly configured and failed to send alarms to the central alarm station. In addition, one card reader’s air compressor PSP card reader was unplugged from its power source which caused the reader to fail to send an alarm to the central alarm station. With respect to CIP-004, a second URE self-reported that it had failed to update the personnel risk assessment (“PRA”) for one of its employees. The URE stated that the employee’s PRA was valid until it expired in the fall. The URE discovered the expired PRA during a quarterly PRA review, resubmitted the PRA, and approximately a month later completed the PRA for the employee.

60. See id.
61. See id.
64. Id.
65. Id.
66. Id.
67. Id.
68. Id.
WECC determined the duration of the violation to be from when the URE should have performed the PRA through when it performed the PRA. 70

For its part, the Commission has issued seven orders approving settlements with Registered Entities, which FERC enforcement staff alleged had violated the mandatory Reliability Standards. 71 Only one of those cases involved alleged violations of a CIP standard. In 2013, FERC’s enforcement staff entered into a settlement with Entergy Services, Inc., which the staff accused of violating CIP-007-1, because the utility allegedly failed to adequately protect critical infrastructure by neglecting to test a firmware upgrade before applying the upgrade in production mode. 72 FERC fined Entergy $975,000, which covered alleged violations of a total of twenty-seven requirements in fifteen standards, not just the violation of the CIP standard, and required Entergy to make semi-annual compliance filings for two years. 73

Finally, with respect to the enforcement of the mandatory CIP Reliability Standards, the Commission affirmed a penalty of $19,500 against the Southwestern Power Administration (“SWPA”), one of four power administrations within the U.S. Department of Energy, for violating CIP-004-1 and CIP-007-1 in 2008-2010. 74 The specific violations, which SWPA did not deny, involved the following activities:

- Two of SWPA’s employees on its authorized unescorted access list had not received 2008 physical security training within 90 days of being placed on the list.

- Two other employees were placed on its access list and given unescorted physical access to a CAA area without a criminal background check being performed within the past seven years.

- Two SWPA contractors were improperly included in the list of personnel with authorized, unescorted physical access to the CA area.

70. Id.
73. See id. at 1-3.
SWPA’s test program for significant changes to Cyber Assets only verified application functionality and did not verify that existing security controls were not adversely affected. SWPA did not test the proper configuration and operation of the security controls.

Dismissing SWPA and DOE’s arguments that the doctrine of sovereign immunity precluded FERC’s imposing a penalty on another Federal agency, the Commission found that the plain language of FPA section 215 explicitly conveys authority to FERC to assess a monetary penalty against a federal entity that is a user, owner, or operator of the Bulk-Power System for a violation of a mandatory Reliability Standard. Among other things, the Commission explained that “any exemption of a large class of customers from the imposition of penalties for violations of a mandatory Reliability Standard would undermine NERC’s enforcement regime, which is an integral part of ensuring the reliable operation of the Bulk-Power System.”

V. POSSIBLE CYBER LEGISLATION AND EXECUTIVE ORDER 13636

For several years, Congress has considered various cyber-security bills, some of which would have expanded FERC’s authority. Partly, these pieces of legislation have been informed by the U.S. Department of Energy Inspector General’s January 2011 audit report on FERC’s “Monitoring of Power Grid Cyber Security.” This report raised concerns about the adequacy of, and the implementation and schedule for, the CIP standards, and concluded that these problems exist in part because FERC’s authority to ensure adequate BES reliability is limited. The audit report then recommended that additional authority be granted to FERC to ensure adequate BES cyber security. FERC staff subsequently testified before Congress, pointing out, among other things, that the standards development process, which takes years and is transparent, is inadequate for the agency to respond timely to a cyber matter, and further is inconsistent with the need to keep security-sensitive information out of the hands of potential adversaries. Accordingly, FERC staff suggested that (1) the Federal government should be able to require mitigation even before or while NERC and its stakeholders develop a standard; when circumstances require urgent action; (2) any legislation should ensure appropriate confidentiality of sensitive information submitted, developed or issued under this authority; (3)

75. Brief of Respondent, supra note 74, at 10.
76. Id. at 32-33.
78. Id. at 2.
79. See id. at 11-12.
Congress should consider extending FERC’s reliability authority beyond the current statutory definition, which does not authorize Federal action to mitigate cyber or other national security threats to reliability that involve certain critical facilities and major population areas; and (4) it is important that entities be able to recover costs they incur to mitigate vulnerabilities and threats.\textsuperscript{81}

With the prospect of legislation being remote in the 113th Congress, President Obama issued Executive Order 13636 (Improving Critical Infrastructure Cybersecurity) (“EO”) in February 2013.\textsuperscript{82} The EO’s stated aim is to strengthen the cyber security of critical infrastructure by increasing information sharing and by jointly developing and implementing a framework of cyber security practices with the government’s industry partners. The EO established new information sharing between the private and public sectors, providing classified and unclassified threat information to U.S. companies.\textsuperscript{83} It required federal agencies to produce unclassified reports of threats to U.S. companies and to share the reports in a timely manner. It also opened up a real-time information sharing program, currently open to the defense industry, to other sectors. In addition, the order directed the National Institute of Standards and Technology (NIST), a federal agency, to develop a new cyber security framework to reduce cyber risks to critical infrastructure, and required NIST to publish a preliminary version of the framework within 240 days of the Executive Order and a final version one year after the Executive Order. Finally, it called on agencies to incorporate privacy and civil liberties safeguards, based in part on the Fair Information Practice Principles, into their cyber security efforts and required agencies to conduct regular, public assessments of their privacy and civil liberties standards.\textsuperscript{84}

In response to the EO, the U.S. Department of Homeland Security created the Integrated Task Force, which consists of eight working groups, each focused on specific implementation deliverables.\textsuperscript{85} As relevant here, NERC and the electric industry experts represent the Electricity Sub-sector on all active implementation working groups. These groups are:

- Cybersecurity Framework Development Working Group, which works with NIST to develop a voluntary, repeatable cybersecurity framework to promote the protection of critical infrastructure;

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{81} \textit{Id.}
\item \textsuperscript{82} Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11739 (2013).
\item \textsuperscript{83} See id. at § 4.
\item \textsuperscript{84} See id. at § 5.
\item \textsuperscript{85} \textsc{N. Am. Elec. Reliability Corp., Agenda: Board of Trustees (Nov. 7, 2013), available at} http://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Minutes%202013/BOT_1113a_Complete%20%28v2%29.pdf.
\end{itemize}
\end{footnotesize}
Cyber Dependent Infrastructure Identification Work Group, which collaborates with industry and the Department of Energy to identify entities with critical infrastructure that, if faced with a cyber incident, could have catastrophic effects;

Planning and Evaluation Work Group, which is tasked with updating the National Infrastructure Protection Plan (“NIPP”) to coordinate public-private efforts to improve infrastructure security and resiliency; and

Incentives Work Group, which directs the study of incentives for participating in the voluntary critical infrastructure cyber-security program.

As an independent agency, FERC is not specifically assigned any responsibilities under the Executive Order. However, shortly before the President issued the Order, on September 20, 2012, the Commission created a new office to focus exclusively on cyber security—the Office of Energy Infrastructure Security (“OEIS”). As described by the FERC Chairman at that time, “[c]reating this office allows FERC to leverage its existing resources with those of other government agencies and private industry in a coordinated, focused manner. Effective mitigation of cyber and other physical attacks requires rapid interactions among regulators, industry and federal and state agencies.”

The office has four primary objectives: (1) to develop recommendations for identifying, communicating and mitigating potential cyber and physical security threats and vulnerabilities to FERC-jurisdictional energy facilities using the Commission’s existing statutory authority; (2) to provide assistance, expertise and advice to other federal and state agencies, jurisdictional utilities and Congress in identifying, communicating and mitigating potential cyber and physical threats and vulnerabilities to FERC-jurisdictional energy facilities; (3) to participate in interagency and intelligence-related coordination and collaboration efforts with appropriate federal and state agencies and industry representatives on cyber and physical security matters related to FERC-jurisdictional energy facilities; and (4) to conduct outreach with private sector owners, users and operators of energy delivery systems regarding identification, communication and mitigation of cyber and physical threats to FERC-jurisdictional energy facilities.

87. Id.
88. Id.
VI. CONCLUSION

As is true for other areas, protection of the nation’s electric grid cyber assets is still in the early stages of development. Unlike other areas, however, this protection is being undertaken within a unique Federally-mandated structure. Congress has charged FERC, an independent regulatory agency, with the responsibility to oversee both the development and the enforcement of standards, which are applicable to over 1,500 entities registered as users, owners, and operators of the Bulk-Power System. FERC fulfills this responsibility by reviewing the actions of NERC and eight Regional Entities, which are required to develop those standards and ensure that the Registered Entities comply with them. NERC is mainly responsible for developing the standards, subject to FERC approval, which it accomplishes through an iterative process in which the electric utility industry is actively involved. The Regional Entities are mainly responsible for enforcing the standards, and may impose hefty penalties, subject to FERC approval, on entities which violate the standards.

To date, FERC has approved over 100 mandatory Reliability Standards. While only about ten percent of those standards pertain to cyber security, the vast majority of the violations discovered and processed since the implementation of the Federal program have involved violations of the cyber infrastructure protection (“CIP”) standards. This fact reflects both the newness of the CIP standards, compared to the other standards, and the concomitant lack of experience of Registered Entities to comply with them. This fact also reflects the high priority that FERC, NERC, and the Regional Entities place on compliance with the CIP standards. There is no reason to believe that their emphasis will change in the future; indeed, more likely they will increase their oversight of protecting critical electric grid cyber assets consistent with the focus of other Federal departments and agencies. Colloquially speaking, “only time will tell” whether the current and relatively new Federal paradigm of developing and enforcing standards is effective, and, if so, whether it is the most effective way to ensure a secure electric grid.
THE CRITICAL ROLE OF EDUCATION IN EVERY CYBER DEFENSE STRATEGY

Juan Cayón Peña, PhD. & Luis Armando García

Abstract: The implementation, maintenance, and improvement of a national Cyber defense strategy involve a range of elements in which education has a predominant role right now. The coordination of both the private and public sectors are needed in order to develop and provide the appropriate curriculum necessary for the principal stakeholders involved in the Cyber defense strategy of any modern nation. This article seeks to identify the challenges faced by these stakeholders, as well as provide recommendations regarding these matters.

I. INTRODUCTION

As computer technology has advanced, both government and private entities have become increasingly dependent on computerized information systems to carry out operations and to process, maintain, and report essential information. Public and private organizations rely on computer systems to develop and maintain intellectual capital, to conduct operations, and to deliver services.¹

Basically, society has become more and more dependent on Information Technology (IT) resources; thus, the protection of these critical assets is increasingly becoming a topic of national interest. Incidents causing disruption of critical infrastructures and IT services can cause major disturbances in the functioning of society. As such, securing cyberspace has become one of the most important challenges of the 21st century for governments. Consequently, Cyber security is increasingly regarded as a “horizontal and strategic national issue affecting all levels of society.”²

This article seeks to describe the role education plays in ensuring Cyber security and Cyber defense on a national level through the proper strategies and/or public policies.

II. CYBER SECURITY STRATEGIES AND ITS RELATION TO CYBER DEFENSE

To some academics, preoccupation with cyber-armed attacks has been counter-experiential up to this point. Yet to others, cyberspace has already become a “full-blown war zone,” and cyber attacks are becoming a “key weapon for governments seeking to defend national sovereignty.” Some of the world’s most prominent nations, including the United States of America (USA), agree that cyber-based threats are evolving and can arise from a wide array of sources. These sources may include business competitors, corrupt employees, criminal groups, hackers, as well as foreign nations engaged in espionage and information warfare. Threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives for acting, which range from monetary gain or political advantage.

On this matter, the British House of Commons Defence Committee made the following conclusion in 2013:

The cyber threat is, like some other emerging threats, one which has the capacity to evolve with almost unimaginable speed and with serious consequences for the nation’s security. The Government needs to put in place – as it has not yet done – mechanisms, people, education, skills, thinking, and policies which take into account both the opportunities and the vulnerabilities which cyber presents.

Given the interconnectivity within cyberspace, a comprehensive approach is called for at both the national and international level, in order to reduce the vulnerabilities a specific nation or group of nations might face. The traditional divisions between military and civilian, public and private, and national and international actors are less clear-cut in cyberspace. National security can, for instance, be jeopardized by a large-scale attack on a private organization. To defend against such attacks, cooperation between different parties is necessary, including the affected organization itself, the intelligence services, the criminal investigation services and, in certain cases, the armed forces as well.

---

5. WSILHUSEN, supra note 1.
As we can see in the following graphic, cyber threat sources range from individual hackers, which pose the least amount of danger, to nation states, which are the most dangerous.8

In response to these and other potential threats, countries began to implement measures to ensure that the IT infrastructures of both the private and public sector would be least exposed. As a result, national Cyber security strategies (CSS) started to become a reality and in some cases, eventually lead to the development later of national Cyber defense strategies (CDS).

According to the European Union Agency for Network and Information Security, a CSS is a tool that improves the security and resilience of national information infrastructures and services.9 It is a “high-level, top-down approach to Cyber security that establishes a range of national objectives and priorities that should be achieved in a specific timeframe.”10

On a similar note, the National Security Framework Manual defines a CSS as “the focused application of specific governmental levers and information assurance principles to public, private, and relevant international ICT systems,

---

9. EUROPEAN UNION AGENCY FOR NETWORK AND INFO. SEC., supra note 2, at 4.
10. Id.
and their associated content, where these systems directly pertain to national security.”

It is important to point out that the understanding of Cyber security tends to vary from country to country, due to the lack of common understanding and approaches between the nations. To this extent, we find that the definition of Cyber security given by the Government of France as a “desired state of an information system in which it can resist events from cyberspace likely to compromise the availability, integrity, or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible,” is the one definition that most relates to Cyber defense.

Nonetheless, it seems clear that the implementation and improvement of CSS comprises a range of elements that usually include documents of political nature, laws, regulations, and administrative measures within a State. Furthermore, training, education, and international cooperation are important features of every CSS in order to function on an operational and tactical level, as we shall demonstrate.

The NATO Cooperative Cyber Defense Centre of Excellence highlights the most relevant CSS and/or CDS drafted to this day, as we can see in the following table:

12. EUROPEAN UNION AGENCY FOR NETWORK AND INFO. SEC., supra note 2, at 9.
14. Compare UNITED NATIONS INT’L. TELECOMM. UNION, http://www.itu.int/en/ITUT/studygroups/com17/Pages/cybersecurity.aspx (last visited Jan. 19, 2014) (defining cyber defense as “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment”), with US DEPT. OF HOMELAND SEC., NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES, http://niccs.us-cert.gov/glossary (last visited Jan. 19, 2014) (defining cyber defense as “the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation”).
15. THE NORTHERN NATION OF PEACE AND SECURITY PROGRAMME, supra note 11, at XVI, 29, 42.
16. See NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, https://ccdcoe.org/328.html (last visited Nov. 19, 2013) (explaining that this organization, established in 2008, is a NATO-accredited International Military Organization dealing with education, consultation, lessons learned, research and development in the field of Cyber security, and is currently sponsored by Estonia, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain and the USA).
17. See id.
<table>
<thead>
<tr>
<th>Country</th>
<th>Year of Cyber security strategy</th>
<th>Cyber defense strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Russia</td>
<td>2000</td>
<td>Yes/2011</td>
</tr>
<tr>
<td>USA</td>
<td>2003</td>
<td>Yes/2011</td>
</tr>
<tr>
<td>Malaysia</td>
<td>2006</td>
<td>Unknown</td>
</tr>
<tr>
<td>Estonia</td>
<td>2008</td>
<td>Yes/2011</td>
</tr>
<tr>
<td>Slovakia</td>
<td>2008</td>
<td>Unknown</td>
</tr>
<tr>
<td>Australia</td>
<td>2009</td>
<td>Unknown</td>
</tr>
<tr>
<td>Canada</td>
<td>2010</td>
<td>Unknown</td>
</tr>
<tr>
<td>Latvia</td>
<td>2010</td>
<td>Unknown</td>
</tr>
<tr>
<td>Poland</td>
<td>2010</td>
<td>Unknown</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>2011</td>
<td>Unknown</td>
</tr>
<tr>
<td>France</td>
<td>2011</td>
<td>Unknown</td>
</tr>
<tr>
<td>Germany</td>
<td>2011</td>
<td>Unknown</td>
</tr>
<tr>
<td>Lithuania</td>
<td>2011</td>
<td>Unknown</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>2011</td>
<td>Unknown</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>2011</td>
<td>Unknown</td>
</tr>
<tr>
<td>New Zealand</td>
<td>2011</td>
<td>Unknown</td>
</tr>
<tr>
<td>South Korea</td>
<td>2011</td>
<td>Unknown</td>
</tr>
<tr>
<td>Uganda</td>
<td>2011</td>
<td>Unknown</td>
</tr>
<tr>
<td>Norway</td>
<td>2012</td>
<td>Unknown</td>
</tr>
<tr>
<td>Switzerland</td>
<td>2012</td>
<td>Unknown</td>
</tr>
<tr>
<td>South Africa</td>
<td>2012</td>
<td>Unknown</td>
</tr>
<tr>
<td>Belgium</td>
<td>2013</td>
<td>Unknown</td>
</tr>
<tr>
<td>The Netherlands</td>
<td>2013</td>
<td>Yes/2013</td>
</tr>
<tr>
<td>Spain</td>
<td>2013</td>
<td>Yes/2013</td>
</tr>
<tr>
<td>Hungary</td>
<td>2013</td>
<td>Unknown</td>
</tr>
<tr>
<td>Italy</td>
<td>2013</td>
<td>Unknown</td>
</tr>
<tr>
<td>Romania</td>
<td>2013</td>
<td>Unknown</td>
</tr>
<tr>
<td>Turkey</td>
<td>2013</td>
<td>Unknown</td>
</tr>
<tr>
<td>Austria</td>
<td>2013</td>
<td>Unknown</td>
</tr>
<tr>
<td>Finland</td>
<td>2013</td>
<td>Unknown</td>
</tr>
<tr>
<td>Montenegro</td>
<td>2013</td>
<td>Unknown</td>
</tr>
<tr>
<td>European Union</td>
<td>2013</td>
<td>Unknown</td>
</tr>
<tr>
<td>India</td>
<td>2013</td>
<td>Unknown</td>
</tr>
<tr>
<td>Japan</td>
<td>2013</td>
<td>Unknown</td>
</tr>
<tr>
<td>Kenya</td>
<td>2013</td>
<td>Unknown</td>
</tr>
</tbody>
</table>
In regards to this list, the following observations are significant:

1. The majority of the strategies were published in the year 2013.

2. Russia and the USA were among the first countries to draft a CSS, subsequently drafting a CDS in the following years.

3. Only five of the thirty-five countries listed have a proper CDS.

4. Normally, the countries that have a CDS previously implemented a CSS, except in the case of Spain, which was almost simultaneously.

Upon the evidence presented so far, it is safe to say that the majority of the countries on the list are most likely to draft a CDS in the very near future, based on the broad goals and objectives of their parent CSS.

Ensuring Cyber security, enforcing rights, and protecting critical information infrastructures require major efforts by the state, both at the national level and in cooperation with international partners. A CSS will only be successful “if all players act as partners and fulfill their tasks together.”

Let us have a look at the role that some of these strategies have placed upon industry and society, relating to the education, training and research of a CSS and CDS.

III. CYBER DEFENSE STRATEGIES AND EDUCATION

The Government of France defined the term cyber defense as “the set of all technical and non-technical measures allowing a State to defend in cyberspace information systems that it considers to be critical.”

Cyber defense capabilities form an important and viable addition to existing military capabilities in that they offer support and reinforcement for operational capabilities in all domains. “These cyber assets strengthen the armed forces’ actions for all military functions, including logistics, command & control, intelligence, force protection, maneuver and firepower.”

In order to develop Cyber defense capabilities, countries must take into account that they cannot be limited to only a national level and must rely upon a “network of allies with whom real-time information can be exchanged on vulnerabilities, protection mechanisms, attacks and countermeasures that can be

19. FRENCH NETWORK AND INFO. SEC. AGENCY, supra note 13, at 21.
20. DUTCH MINISTRY OF DEFENCE, supra note 7, at 8.
implemented against cyber-attacks led directly or indirectly by States or terrorist groups."\(^{21}\)

Furthermore, effective mitigation against the threat of cyber-attack can only come from a combination of technical and nontechnical measures. Technical mitigation techniques can include firewalls and network intrusion detection. Nontechnical mitigation usually combines leadership, education, and policy development. “An effective Defense against the ever-evolving threat can only be achieved through a balance between these two complementary techniques.\(^{22}\)

In 2011, the United States Department of Defense identified five strategic initiatives involving cyberspace and the national Defense strategy.\(^{23}\) Strategic initiative five strived to “leverage the nation’s ingenuity through an exceptional cyber workforce and rapid technological innovation,” in line with the following statement:

> The defense of U.S. national security interests in cyberspace depends on the talent and ingenuity of the American people. DoD will catalyze U.S. scientific, academic, and economic resources to build a pool of talented civilian and military personnel to operate in cyberspace and achieve DoD objectives. Technological innovation is at the forefront of national security, and DoD will foster rapid innovation and enhance its acquisition processes to ensure effective cyberspace operations. DoD will invest in its people, technology, and research and development to create and sustain the cyberspace capabilities that are vital to national security.\(^{24}\)

Education in Cyber security and Cyber defense settings will normally be linked to research and development (R&D), as is the case for the USA and the European Union (EU). In the EU, the European Agency for Network and Information Security stated in 2012 that European universities and R&D institutions do not produce enough Cyber security experts to meet the increasing needs of this sector. Therefore, the objectives of a training and education program within the EU could include the following:

\[\text{\cite{french-network-and-info-sec-agency}, \cite{alan-baldwin-john-palfreyma}, \cite{us-dept-defense-department-defense-strategy-operating-cyberspace}.}\]


\(^{22}\) Alan Baldwin & John Palfreyman, supra note 8, at 3.

\(^{23}\) U.S. Dept. of Defense, Department of Defense Strategy for Operating in Cyberspace 5-10 (2011), available at www.defense.gov/news/d20110714cyber.pdf. (identifying the following: Strategic Initiative 1: Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace’s potential; Strategic Initiative 2: Employ new Defense operating concepts to protect DoD networks and systems; Strategic Initiative 3: Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government Cyber security strategy; Strategic Initiative 4: Build robust relationships with U.S. allies and international partners to strengthen collective Cyber security; Strategic Initiative 5: Leverage the nation’s ingenuity through an exceptional cyber workforce and rapid technological innovation).

\(^{24}\) Id. at 10.
1. To enhance the operational capabilities of the existing information security workforce.

   Action: Create a national register with accredited Cyber security experts with teaching skills.

2. To encourage students to join and then prepare them to enter the Cyber security field.

   Action: Add information security courses to university curricula, not only to the ones related with computer science but also to any professional specialty tailored to the needs of that profession.

3. To promote and encourage the relations between information security academic environments and the information security industry.

   Action: Support the security accreditation and certification of skilled personnel in key working posts in every industrial sector.

Similarly, the Czech Republic CSS of 2012 stated the following on education and training programs:

   Cooperation aimed at creating training programmes focusing on cybernetic security shall be started with the academic and private spheres. Needs for qualification in cybernetic security, opportunities of school and other education shall be evaluated on a regular basis. The issue of cybernetic security will be implemented into all levels of education.25

The implementation of Cyber security awareness into all levels of education seems to be one of the focal points of the Czech strategy. The Hungarian CSS of 2013 points in this direction as well, revealing a slight trend within the EU:

   Education, research & development: Hungary pays particular attention to integrating cyber security as a field in the information technology syllabus of primary, secondary and higher education, in training courses for government officials and in professional retraining courses. Hungary strives for strategic cooperation with university and scientific research locations which have achieved outstanding and internationally

recognised results in cyber security research and development and help establish cyber security centres of excellence.26

Also in this direction, the Government of France stated that the long-term objective in their CSS is to “raise citizens’ awareness of Cyber security issues during the education process,” requiring the “implementation of an active governmental communication policy.”27

On a similar note, the Dutch CDS acknowledges the importance of Cyber security awareness, stating that “all defence personnel must be aware of the risks associated with the use of digital assets.”28 Cyber security awareness will become an integrated part of all defense training courses. To this extent, cooperation with public-sector partners, universities and the private sector will be needed in the areas of R&D and training.29

High education institutions, especially universities, will play a prominent role in achieving all of this. That is why the Government of Norway identified in its CSS seven strategic priorities, one of them being the “high quality national research and development in the field of information security” in which all stakeholders should strive to facilitate productive interaction between leading ICT companies and academic environments across sectors.30

Another example is the British CSS published in 2011 which drafted an action plan that included the encouragement, support, and development of education at all levels, as well as crucial skills and R&D.31 Specifically, the strategy looked to establish certification programs for cyber security professionals through postgraduate education.32

Based on an interview that the authors of this article had with the commanding General Carlos Gómez López de Medina, the Spanish Joint Cyber Defense Command, which was created in 2013 and which coordinates the Spanish CDS,33 is developing a Master’s Degree in Cyber Defense along with several Spanish public institutions, including the Ministry of Defense. This effort

27. FRENCH NETWORK AND INFO. SEC. AGENCY, supra note 13, at 14.
28. DUTCH MINISTRY OF DEFENCE, supra note 7, at 9.
29. Id. at 15.
32. Id. at 42.
is in addition to the Cyber defense training programs they are set to develop in 2014 for their personnel, focused primarily on military Cyber security expertise.

Finally, the Indian CSS that was published in 2013 established in the following goals, found in objective J regarding “Human Resource Development”:

1. To foster education and training programs both in formal and informal sectors to support the Nation’s Cyber security needs and build capacity.

2. To establish Cyber security training infrastructure across the country by way of public private partnership arrangements.

3. To establish Cyber security concept labs for awareness and skill development in key areas.

4. To establish institutional mechanisms for capacity building for Law Enforcement Agencies.34

IV. CHALLENGES AND RECOMMENDATIONS

As we have seen, the implementation, maintenance and improvement of a national CDS involves a range of elements in which education has a predominant role right now.

The coordination of both the private and public sectors is needed in order to develop and provide the appropriate curriculum needed for the principal stakeholders involved in the CDS of any modern nation.

Some of the challenges faced by these stakeholders are:

1. Ensuring the trust and cooperation of other countries.

2. Integrating Cyber security awareness in all levels of education.

3. Promoting the development of Cyber security professionals.

4. Ensuring cooperation between state, industry, and society.

In order to overcome these challenges, we recommend the following:

a) Involvement of higher education and R&D institutions, both public and private, in the drafting and implementation of CSS and CDS.

b) Clear, specific and short term goals for CSS and CDS.

c) Sharing of knowledge and information with the general society towards the goals of CSS and CDS.
INFORMATION SECURITY CHALLENGES FOR COMPANIES IN THE DIGITAL AGE

Ors Penzes

ABSTRACT

The objective of the article is to provide some guiding thoughts, simulative approaches, and feasible, inspirational analogies for theoretical professionals and practicing decision-makers alike (including business, legal, security, and military strategists, as well as analytical and information technology experts). These analogies and techniques (1) may help identify high-risk companies (especially when companies are seeking new business partners), and (2) may be used as input for different on-going research (regarding security and threat assessment).

Due to the ability of businesses and governments to collect, store, and readily access limitless amounts of data, the classic phrase “knowledge is power” has become “information is power.” 1 If this author could freshen up the phrase even further, it would be “checked and verified information is real power.”

I. IN ONLY 24-72 HOURS

Operating from a small office abroad, a company can move tons of material without physically seeing the ships, having any personal acquaintance with the management of the partner company, or witnessing the delivery process itself. With just “the click of a button,” we can buy and sell worldwide.

Thanks to technological innovation and free trade agreements, 2 geographical boundaries and distances have practically been eliminated and national barriers have been reduced. This has expanded the already huge business playing field and, as such, the world has become a “global village.” 3 But this phenomenon is largely based upon the fast information flow we currently enjoy.

1. See, e.g., ANDREJ HUCZYNSKI, INFLUENCING WITHIN ORGANIZATIONS 331 (2d ed. 2004) (referencing that “Francis Bacon said that ‘knowledge is power,’” but that today “[i]nformation is power” for businesses); Simon Rogers, Information is power, THE GUARDIAN (May 23, 2010), http://www.theguardian.com/media/2010/may/24/data-journalism (noting access to government information is power for journalists). See also, David Cay Johnston, Glenn Greenwald and the Future of Leaks, NEWSWEEK (Oct. 25, 2013, 5:05 PM), www.newsweek.com/glenn-greenwald-and-future-leaks-758 (discussing the current controversies involving the collection of data by government and businesses and access to that data by citizens through leaks).

2. See Free Trade Agreements, INT’L TRADE ADMIN., http://trade.gov/fta/ (last visited Mar. 22, 2014) (“Free Trade Agreements (FTAs) have proved to be one of the best ways to open up foreign markets to U.S. exporters. Trade Agreements reduce barriers to U.S. exports, and protect U.S. interests . . . . In 2012, 46 percent of U.S. goods exports went to FTA partner countries . . . [which] totaled $718 billion . . . .”).

The radio (one of the oldest modern information networks) reached approximately 60 million people in its first 30 years. Television broadcasts reached the same amount of people in 15 years. The Internet has grown almost 10 times faster than any of the above media mentioned. In 1984, the number of hosts was 1,000. The number of hosts exceeded 10,000 in 1987 and 100,000 in 1989. By 1992, the number of hosts was more than 1,000,000.

The improvements in technology, the Internet, technological connectivity, e-business, and e-government have all boosted international business: making it faster, more flexible, cheaper, and easier to conduct than ever before. We can bridge the oceans with our technological networks, and thus, personal interaction is no longer as important in the business environment. However, on this huge field there are numerous players; new and unknown companies are emerging every day, and the reliability and transparency of companies or individuals has become more and more questionable. Many small, unheard of, but well-performing companies have become accessible thanks to the above-mentioned

(discussing Marshall McLuhan’s theory of a “global village,” where everyone around the world is connected and linked through communication technology. Even before McLuhan’s death in 1955, he recognized that “[t]he age of civilization has ended, and that of one civilization . . . is beginning.”).

4. Robert D. Hof, Gary McWilliams, & Gabrielle Saveri, Overview: The “Click Here” Economy, BUSINESS WEEK (June 11, 1998), http://www.businessweek.com/1998/25/itspec98.htm (“Without a doubt, the Internet is ushering in an era of sweeping change that will leave no business or industry untouched. In just three years, the Net has gone from a playground for nerds into a vast communications and trading center where some 90 million people swap information or do deals around the world. Imagine: It took radio more than 30 years to reach 60 million people, and television 15 years. Never has a technology caught fire so fast.”).

5. Id.

6. Id.


8. Id. at 2-3.

9. Id. at 4.


11. See, e.g., Mitchell A. Petersen & Raghuram G. Rajan, Does Distance Still Matter? The Information Revolution in Small Business Lending, 57 J. FIN. 2533, 2566 (2002) (concluding that financial institutions are working with more distant lenders, while at the same time, the communication between these distant parties is less personal).

12. See, e.g., Carol Kinsey Goman, Five Signs That Your Company Is Fraudulent, FORBES (June 11, 2013, 2:52 PM), http://www.forbes.com/sites/carolkinseygoman/2013/06/11/five-signs-that-your-company-is-fraudulent/ (providing “red flags” of fraudulent companies, as found in Bre-X Minerals, Enron, and Bernie Madoff’s Ponzi scheme. The five “high alert” signals when assessing a company are: (1) controlled access to evidence, (2) inconsistencies in evidence, (3) authority bias, (4) intense focus on the market, and (5) too good to be true).
advances, and conducting businesses with them can be extremely beneficial. But the question arises: who really stands behind an offer or business proposal coming from somewhere in the other hemisphere of the globe?

The game of international business is fast, vast, and open. Each computer connected to the Internet can have direct contact with other computers, and in international trade, each company can conduct business with any number of other companies. In a system where everybody can contact everybody else, risk is increased. “Simple” or “closed” structures are more secure; conversely, “open-systems” are more insecure. Safety requires transparency and regulated structures. Insecurity increases with the complexity of the relations.

We have never had a medium prior to the Internet, be it phone or fax, which could contact a number of companies so easily. For this reason, these networks are

---

13. See, e.g., Greg Satell, 5 Exciting Tech Companies You’ve Probably Never Heard Of, FORBES (July 23, 2013, 8:06 AM), http://www.forbes.com/sites/gregsatell/2013/07/23/5-exciting-tech-companies-youve-probably-never-heard-of/ (profiling five exciting - yet mostly unknown - companies impacting the future of technology). The rise of these type of companies, in contrast to industry giants like Apple and Google, is possible because “[a]s digital technology reduces the importance of borders, we’re going to see more companies . . . build great businesses in developing markets that can compete as global giants.”).


16. See WORLD HEALTH ORG., supra note 16.

17. Josh Baskin, Note, Competitive Regulation of Mobile Software Systems: Promoting Innovation Through Reform of Antitrust and Patent Laws, 64 HASTINGS L.J. 1727, 1729 (2013) (“Open systems allow broad compatibility between many different devices. Closed systems, on the other hand, tend to limit access between parts through specific rules or only allow preapproved components to connect to the system in the first place . . . . In an ideal world, regulators would seek open and stable systems, which provide the greatest potential for innovation while maintaining security, privacy, and stability. In the real world, there is a trade-off between allowing openness (or maximum compatibility and customizability) and providing security, stability, and protection for rights-holders, which in its own right spurs more innovation.”).

18. Id.

exponentially more vulnerable (and the multitudes of unscrupulous opportunists make it even more unsafe).^{20}

Getting information is easy, because much of what happens in the world or global business can be read and seen online anywhere, within less than a minute.^{21} The information is all around us—in the here and now. The problem is not in gathering information about companies, but in obtaining the data that is most important.^{22} This “click of a button” access and interdependence brings about other threats such as misleading data, free riders, and fake companies.^{23} A business should conduct a classic verification process of new business partners: check the commercial register, website, tax-number, bank account number, etc.^{24}

While each country requires specific procedures to create a new business,^{25} a clever, fake company may provide all of these items.^{26} In many countries, a company can be created via e-government within 24-72 hours.^{27} Via the Internet, a company may easily register for a domain and open a bank account.^{28} Within a

\[\text{20. See, e.g.}, \text{ VERIZON, 2013 DATA BREACH INVESTIGATIONS REPORT 19 (2013), available at http://www.verizonenterprise.com/DBIR/2013/) (reporting the results of a study that analyzed more than 47,000 reported security incidents from 2012).}\]
\[\text{22. See, e.g., Kenneth Coats, WHY YOU SHOULD BACKGROUND CHECK YOUR BUSINESS PARTNER, HUFFINGTON POST (Dec. 17, 2013, 6:17 PM), http://www.huffingtonpost.com/kenneth-coats/why-you-should-background_b_4462216.html (“When it comes to starting a business, nothing is more important than picking the right people to work with. What may seem like an invasion of privacy could be what ultimately protects you and your startup from ruin.”).}\]
\[\text{24. Verification services vary by country. E.g., Sally Darby, HOW CAN I CHECK IF A COMPANY IS LEGITIMATE?, MONEY.CO.UK, http://www.money.co.uk/article/1004946-how-can-i-check-if-a-company-is-legitimate.html (last visited Apr. 6, 2014) (providing verification methods and websites for the United Kingdom).}\]
\[\text{27. Time Required to Start a Business (Days), THE WORLD BANK, http://data.worldbank.org/indicator/IC.REG.DURS?order=wbapi_data_value_2013+wbapi_data_value-last&sort=asc (last visited Apr. 13, 2014) (providing a list of countries with “the number of calendar days needed to complete the procedures to legally operate a business.”). New Zealand, Macedonia, Rwanda, Georgia, Singapore, Australia, Portugal, and China, all allow business creation and operation to occur in three days or less. Id.}\]
short timeframe, a company can buy, sell, or purchase goods and services worldwide. A large portion of selling, buying, logistics, operations, and marketing of goods and services are already done via networks between companies, between intangible and personally unseen management.

At first sight, a businessperson cannot be sure whether a partner-company’s activity is legitimate. There is no way to be absolutely confident that a domain name (with the same company name) belongs to the company or not. When the phone number of a company is called, one cannot be 100% certain of the manager’s identity. Does the seat of the company exist at all? Is there even a number twenty-three on the given street somewhere in Fez or Odessa? Is there a 5th floor in the building where the company has been seated, or does the building only have four floors? Or have the shareholders assigned the ownership of the shares to a penniless scapegoat?

For example, a nine-year-old child from Macao could create a web page by registering the www.maxle.biz domain at an Indonesian domain portal. First, the company may not exist at all. Second, even if Maxle Company does exist, it may not know about the existence of the child’s webpage. Thus, any business dealing with Maxle Company through www.maxle.biz would be doing so at its own peril.

---

29. See THE WORLD BANK, supra note 27.
31. See Shopping Safely Online, BETTER BUS. BUREAU (Mar. 25, 2003), http://www.bbb.org/us/article/shopping-safely-online-407 (“By using widely available tools which can easily copy or recreate digital graphics, a computer-literate cyberspace crook can build a website that looks strikingly similar to that of a legitimate online business.”).
32. While there are many services that identify the owner of a website URL by providing the owner’s name, IP address, and address, these services, not only fail to verify the information, but they also frequently list owners as “private.” See Protect Your Privacy with Private Domain Registrations, WORDPRESS.COM, http://en.blog.wordpress.com/2010/07/30/private-domain-registrations/ (last visited Apr. 13, 2014) (describing how users can upgrade their domain registration to maintain their privacy). See generally CHECKDOMAIN.COM, http://www.checkdomain.com/ (last visited Mar. 31, 2014) (providing an online service to identify domain ownership).
II. ON THE WAY FROM OFF-LINE TO ON-LINE

A few decades ago, business people knew each other personally or by reputation. They knew who, where, in which market, and in which business area their colleagues operated or had an interest. I am not proposing that this personal relation filtered out all possible frauds, of course not, but the “friend of a friend” relationship reduced the fraud risk. Personal interaction is no longer so important in the business environment. Nowadays, parties are commonly unidentified because they are geographically separated from each other; and this kind of “anonymity” and “geographical distance,” can affect their behavior adversely. Let’s see a simple example: if I do not pay back a loan to my neighbor, I will listen to his maledictions for the next 30 years. If an individual could choose from two creditors, he would more likely pick somebody who lives in the next county, rather than his neighbor. In 2012, consumers submitted

---


35. See THE OXFORD HANDBOOK OF INTERNET PSYCHOLOGY 295 (Adam Joinson et al. eds., 2007) (“[B]ecause people report valuing authenticity and trust in close relationships, people tend to lie less to close relationship partners, such as spouses, family and friends, than to casual relationship partners, such as acquaintances, colleagues and strangers . . . . [L]ies told in close relationships tend to be more altruistic, in which the lie is told primarily to benefit the target (e.g., false compliments, pretend agreement) than self-serving, in which the lie benefits the liar, while lies in casual relationships tend to be more self-serving than altruistic.”). But see id. at 292 (“[C]omparing identity fraud that took place online or [face-to-face] suggests that identity fraud is still much more likely to take place [face-to-face], and that when it does occur online it tends to be much less costly than when it occurs offline . . . .”).


37. See THE OXFORD HANDBOOK OF INTERNET PSYCHOLOGY, supra note 35, at 292 (“[M]ore serious and criminal forms of deception are keeping pace with the increase in money flowing through the internet . . . . [T]he Internet offers a highly flexible environment for identity-based forms of deception that can make it difficult for even technologically savvy users to detect deception.”); NAT’L WHITE COLLAR CRIME CTR., INTERNET FRAUD 1 (2013), http://www.nw3c.org/docs/whitepapers/internet_fraud.pdf?sfvrsn=8 (“The Internet is an appealing medium for committing crime because it allows anonymous contact with a large pool of victims without incurring significant cost.”). See generally Pankaj Ghemawat, Distance Still Matters: The Hard Reality of Global Expansion, HARV. BUS. REV., Sept. 2001, at 137-38 (“Much has been made of the death of distance in recent years. It’s been argued that information technologies and, in particular, global communications are shrinking the world, . . . . [b]ut when it comes to business, that’s not only an incorrect assumption, it’s a dangerous one. Distance still matters, and companies must explicitly and thoroughly account for it . . . .”).
289,874 complaints to the United States’ Internet Fraud Complaint Center; these complaints represent a total loss of $525 billion.

III. IF YOU STEP INSIDE THE ROPES, YOU CAN COUNT ON PUNCHES

On one hand, globalization works as a “collective benefit” with plenty of networks (from telecommunications to infrastructure). We count on open access to these networks for their relative lack of expense; everybody benefits from their usage, like a free, endless highway. While businesses want to sustain the Internet, most businesses do not want to spend money and time to make the Internet safer and more organized. The open-flowing nature of the Internet, combined with the legal ramifications and security risks from global e-commerce, are analogous to the clichés: “when in Rome, do as the Romans do,” but caveat emptor (“let the buyer beware”). The borderless nature of the Internet has important international legal ramifications.

Before conducting global e-business, a business needs to recognize the possible consequences. Unless “operations are limited exclusively to domestic consumers, any entity engaged in e-commerce must be aware of cross-border legal issues.” Global e-business is not a friendly, late afternoon tea party; instead, if you step inside the ropes, you may get hit.

39. Id.
40. See Katherine Yester, Measuring Globalization, FP (Jan. 1, 2001), http://www.foreignpolicy.com/articles/2001/01/01/measuring_globalization (discussing an increase in the online population and the number of international travelers while also discussing the benefit of globalization).
41. See George Sadowsky, The Internet Society and Developing Countries, ON THE INTERNET, (Nov./Dec., 1996), http://www.isoc.org/oti/articles/1196/sadowsky.html (“The correlation between information, communication, and economic growth is well-known, making the usefulness of networks nearly self-evident. Electronic networking is a powerful, rapid, and inexpensive way to communicate and to exchange information.”).
45. See Matthew Wilson, Reducing Legal Risks: Online Commerce, Information Security, and the World, 33 WYO. LAW. 24, 25 (2010) (“The great potential of e-commerce is accompanied by many complicated legal issues including the enforceability of online commercial obligations, the recognition of personal rights, virtual criminal acts, and many others.”).
46. Id.
47. Id.
IV. I FOLLOW THE RULES—CAN I ASSUME THAT THE OTHER PLAYER DOES THE SAME?

There are a few areas where the members of a group can work smoothly together with different national, cultural, and political backgrounds. For example, there are universally recognized standards in mathematics, physics, road traffic, the Internet, and global business. These are areas where people accept more or less the same “collective principles” regardless of their biases.

One such principle in business is that each party assumes that dealing is better than not dealing. “I can sell if somebody wants to buy; I need to deal with others to gain more benefits in my business” (like in a game theory). The possibility of mutual gain exists. When working toward mutual benefit, the different cultural core values, beliefs, and views are bridgeable. The benefit is achievable only through co-operation. From the “prisoner’s dilemma” strategy aspect, everybody chooses “cooperation” instead of “defection.”

48. See generally Joel L. Sachs et al., The Evolution of Cooperation, 79 Q. REV. BIOLOGY 135, 136 (2004) ("[There are] three general models by which cooperation can evolve and be maintained: (i) directed reciprocation -- cooperation with individuals who give in return; (ii) shared genes -- cooperation with relatives (e.g., kin selection); and (iii) byproduct benefits -- cooperation as an incidental consequence of selfish action."); Joel Sobel, Can We Trust Social Capital?, 40 J. ECON. LITERATURE 139, 139 (2002) ("Social capital describes circumstances in which individuals can use membership in groups and networks to secure benefits.").

49. See Sachs, supra note 48, at 145 (“One general class of byproduct mutualism is synergism: actions or coordinated behaviors that are automatically more profitable when performed in groups . . . ”).

50. See, e.g., id. at 146 (“When one individual (Y) receives automatic byproduct benefits from another individual (X), natural selection can shape Y to maximize these benefits by being cooperative toward X.”).

51. 5A OHIO JUR. 3D ALTERNATIVE DISPUTE RESOLUTION § 29 (3d ed. 2014) (“Game theory is a means of determining the optimal solution in conflict, independent of the problems of assessing the credibility of parties’ threats, promises, or arguments. Game theory attempts to offer guidance concerning what choices and assumptions about the other’s behavior ought to be made based upon the payoff associated with each combination of a player’s choices, and based on the assumption that the parties will act rationally to maximize gain and minimize loss. It is an approach for modeling situations of conflict by assuming certain interactional components (players, moves, payoffs, strategies, and rules) as an aid to clarifying negotiating alternatives that are available to a negotiator and an opponent.”); David Crump, Game Theory, Legislation, and the Multiple Meanings of Equality, 38 HARV. J. ON LEGIS. 331, 331 (2001) (“Game theory is the study of strategic interactions that can be analyzed by logic.”).


53. See Moshe Hirsch, Game Theory, International Law, and Future Environmental Cooperation in the Middle East, 27 DENV. J. INT’L L. & POL’Y 75, 76 (1998) (“Attaining optimal results in an interactive situation frequently requires ‘collective action.’ Collective action occurs when the efforts of two or more individuals are needed to achieve a certain outcome, one which will typically further the interests or well-being of the group.”).

54. See Daniel Donovan & John Rhodes, The Prisoner’s Dilemma Becomes the Lawyer’s Dilemma: To Be a Zealous Advocate or a Judas Goat?, 35 MONT. LAW. 8, 9-11 (2010) (explaining the “prisoner’s dilemma,” as when “two players may each cooperate with or betray the other player.” For example, imagine there are two suspects, each held in a separate interrogation room.
For example, it is beneficial for a driver to accept the general principle of traffic regulation. This means not to drive the opposite direction down a one-way road. Further, it is obvious, for example, not to use the symbol “6” instead of the symbol “3” if I want communicate clearly, and if I want the other person to understand the same as I do. If players are rational actors, they assume that the other party accepts the mutual rules, and all players act on the minimum level of good faith. This kind of psychological thinking drives to reciprocity: “If I follow the rules, I can expect others to do the same.”

Therefore, business relies on a minimum level of trust. Without common trust, there is no business: “I trust my partner and have a reason to believe that the agreement is more or less achievable. I assume that the other business person thinks in the same way or at least similarly.” Companies try to ensure and clarify their beliefs in different ways: by obtaining agreements, indemnities, warranties, juridical authorities, letters of credit, and other forms of documentary evidence. Fraudulent and deceptive companies often assume that others will trust them. Moreover, fraudulent companies can obtain a significant benefit if they decide to act illegally or unethically (by becoming an immoral opportunist). The non-materialized benefit is trust, the materialized benefit is money or resources.

without the ability to communicate with the other. Each suspect may remain silent, confess, or implicate the other suspect. Possible scenarios include: (1) both suspects implicating the other, (2) both suspects remaining silent, or (3) one suspect implicating the other, while the other suspect remains silent. Not only do the scenarios present different verdict possibilities, but they also may result different punishment. If both suspects act selfishly and implicate the other suspect, they will most likely both receive longer sentences than if they both cooperated with the other by remaining silent).

55. See Paul N. Cox, The Public, the Private and the Corporation, 80 MARQ. L. REV. 391, 432 (1997) (“The notion is that, in contexts of human interaction, gains from cooperation are possible . . . [F]or example, that a rational person[] will cooperate (‘trust’ in the sense of ‘risk defection’) if (1) the gain he expects from mutual cooperation exceeds the payoff from expected mutual defection (non-trust or non-cooperation), and (2) he assigns a sufficiently high probability of cooperation from the other(s) engaged in the interaction.”).

56. See id. at 483-84.

57. David DeSento, Who Can You Trust?, HARV. BUS. REV., Mar. 2014 (“Success in business unquestionably requires some willingness to cooperate with and have faith in others.”).

58. See Roderick M. Kramer, Rethinking Trust, HARV. BUS. REV., June 2009 (“For the past two decades, trust has been touted as the all-powerful lubricant that keeps the economic wheels turning and greases the right connections—all to our collective benefit.”).

59. See generally ROBERT A. FELDMAN & RAYMOND T. NIMMER, DRAFTING EFFECTIVE CONT. § 5.06 (2014) (providing an overview on risk allocation in contracts).

60. See, e.g., DeSento, supra note 57 (“On the surface, Madoff possessed all the bona fides—the record, the résumé, the expertise, and the social connections. But the fact that so many people, including some sophisticated financial experts and business leaders, were lulled into a false sense of security when dealing with Madoff should give us pause. Why are we so prone to trusting?”). Id. (“[H]uman beings are naturally predisposed to trust—it’s in our genes and our childhood learning—and by and large it’s a survival mechanism that has served our species well. That said, our willingness to trust often gets us into trouble. Moreover, we sometimes have difficulty distinguishing trustworthy people from untrustworthy ones.”).

61. See id.
V. THE ELIMINATION OF SKEPTICISM

Through daily routines, we get used to trusting in common things. For instance, I can take it for granted that if I put the number 345 into an on-line calculator, and multiply it by 456, the result will be 157,321. We can take for granted that the domain name “Shell” belongs to the oil company. These are logical occurrences.

We have learned to skip over checking data in our fast-paced world. We take for granted some things; however, these can make us “un-skeptical” and naive in our daily lives and in the business world, as well. Moreover, when an individual checks facts, it is unlikely that the individual will validate credible information more than once. The number 345 multiplied by 456 is not 157,321, but is actually 157,320. The domain “Shell.de” did not belong to the multinational oil company until a few years ago, but to an “unrelated” third person.

VI. LEGAL RESPONSES? BOUNDARIES OF THE LAW?
ARCHAIC AND PREJUDICIAL-AGE?

If an unlucky situation occurs, legal implications are almost certain to follow. However, sometimes these results are not business-like: the time and money wasted are regrettable. First, the law is not a silver bullet; prevention is not the primary objective of the law. Law can handle—merely—the
consequences (like illegal benefit, damages, fraud, etc.).\textsuperscript{69} The approaches of legal processes are almost always retrospective, and not preventative.\textsuperscript{70} The aim of the law can be deterrence and restitution: the re-establishment of the original situation before the illegal action was taken.\textsuperscript{71} These are the natural boundaries of the legal systems; in a cynical way one could say: “We are unable to ask a police officer to guard each individual business transaction.”

Second, the situation is controversial because in some cases the “symptoms” are so close to each other (business delay v. fraud) that we do not know what is going on behind the scenes.\textsuperscript{72} In several legal systems, these are two different processes (private law and criminal law); therefore, the proceeding, the authorities, and the legal ways are different, which cause natural delays.\textsuperscript{73}

Third, if the companies are seated in different countries and cultures, several legal systems and multiple jurisdictions can be involved, which make cases more difficult.\textsuperscript{74}

Fourth, the final outcome can never be taken for granted because of the quasi, and/or semi-quasi, legal boundaries and limitations (e.g., liquidity, insolvency, international aid, homeless owner, under-age, incapacity, de-registration, procedural delay, etc.).\textsuperscript{75} Turning back to the before mentioned scenario, it might be difficult to execute any final judgement against the child culpable individuals, as opposed to those intended simply to extract compensation or restore the status quo, were issued by courts of law, not courts of equity.

\textsuperscript{69} See id.

\textsuperscript{70} See, e.g., Emhart Corp. v. USM Corp., 527 F.2d 177, 183 (1st Cir. 1975) (“We can agree that an ounce of prevention is better than a pound of cure, but the very fact that cure is available militates against a pound of prevention before the patient is sick.”).

\textsuperscript{71} Benjamin R. Civiletti & David W. Goewe, 4 Bus. & Com. Litig., Fed. Cts. § 44:17 (3d ed. 2013) (“The principal goal of a compensatory damage award is to make the plaintiff ‘whole.’ The injured party should be placed in the position it would have occupied had the unlawful conduct not occurred.”).

\textsuperscript{72} See, e.g., In re Wreyford, 505 B.R. 47, 55 (Bankr. D.N.M. 2014) (discussing the meaning of delay and fraud in the bankruptcy context).

\textsuperscript{73} See generally Edward R. Bonanno, Parallel Proceedings Issues for Criminal and Civil Enforcement, N.J. Law., Feb. 2005, at 17 (“Parallel proceedings are simultaneous or concurrent criminal, civil or administrative enforcement actions that target the same violator at the same time for the same or similar offenses. Many federal and state statutes that address health, the environment, and public welfare authorize the government to conduct both civil and criminal investigations, and to seek both civil/administrative and criminal sanctions.”).

\textsuperscript{74} Anthony J. Colangelo, Universal Jurisdiction As an International “False Conflict” of Laws, 30 Mich. J. Int’l L. 881, 888 (2009) (“[I]nternational law contains multiple bases of national jurisdiction. These bases of jurisdiction derive from a state’s independent national entitlements as recognized by international law; namely, the state’s entitlement over its territory, its entitlement to punish and protect its nationals, and its entitlement to secure itself as a State. Moreover, when States seek to regulate activity falling within the compass of their national jurisdiction, they largely are free to employ their domestic lawgiving apparatus however they see fit by defining offenses according to their own individual—and independent—prescriptive prerogatives.”).

\textsuperscript{75} Ann Taylor Schwing, 2 Cal. Affirmative Def. § 31:7 (2d ed. 2014) (“The remedy at law may be inadequate even if damages can be proved to the penny if the defendant to be held liable for the damages is insolvent . . . . Similar inadequacy of the remedy at law arises when the defendant is judgment proof for another reason, such as immunity from suit for damages.”).
from Macao because he cannot be punishable, etc.\textsuperscript{76} Maybe the fraudsters using the domain name registered by the child could be found, the judgement would be executable, and the assets recovered. However, the process might be too long, the costs might be too high, and the solution might not be beneficial based on a cost-benefit analysis. The company’s non-material or material losses might not be comparable with the benefit of the final judgement or with the final legal outcome. Therefore, the most viable and business-like solution is prevention.\textsuperscript{77}

\section*{VII. Simulations—By Way of Conclusion}

This author thinks that there are several different methods to ensure the validity of the data received. The following are simple, but implementable simulations.

\textit{A. Birth-Mark}

\textit{Poničan} is a Slovak ballad about a mother who recognizes her son after not seeing each other for decades.\textsuperscript{78} The Turks had a tradition of “stealing” young children from their enemies. They would then raise the children as their own with Turkish traditions, but they called them Janissaries among each other.\textsuperscript{79} In this ballad, a Turkish Janissary soldier captured one old woman and made her his domestic slave in order to take care of his son.\textsuperscript{80} Decades later, the old woman recognized the birthmark of her stolen son on the soldier’s back and started to sing the story of the family to her grandchild.\textsuperscript{81} The birthmark was a definable, unique, and unmistakable fixed point.\textsuperscript{82} We already use and know various kinds of “birthmarks”: iris-recording, fingerprints, DNA (deoxyribonucleic acid), DNS (domain name system), chips, natural signatures, electronic-signatures, places of organization, and account numbers that work in much the same way—as fixed points.

\textsuperscript{76} See infra Part I.
\textsuperscript{77} See, \textit{e.g.}, Internet Fraud, USA.GOV, http://www.usa.gov/Citizen/Topics/Internet-Fraud.shtml (last visited Apr. 19, 2014) (“The best way to fight internet fraud is to learn how to avoid becoming a victim.”).
\textsuperscript{78} Romanticism, The CTR. FOR INFO. ON LITERATURE, http://www.litcentrum.sk/31587 (last visited Apr. 5, 2014) (“Poničan” takes its subject from the Turkish raids on Slovakia, during which the Turkish squads not only pillaged, murdered, but also took children prisoner and brought them up in Turkey to be tough and ruthless warriors against the national communities they came from. This attribute of theirs became a Slovak saying: Better a Turk than a janissary. Chalupka gave his story about a ‘janissary’, who came from Poniky (therefore Poničan) another dimension: a Slovak boy who was brought up as a soldier in Turkey returns to Poniky and his grandmother recognises him because of a birthmark. His native blood responds and so the poem ends as an idyll.”).
\textsuperscript{79} Id.
\textsuperscript{80} Id.
\textsuperscript{81} Id.
\textsuperscript{82} Id.
B. Birth-Mark—Different Sources

The fixed-point is unique, and unmistakable. However, we may check the position of a fixed-point only with other fixed-points. If the “information database” is based on incorrect input-information, we cannot figure out the fraud in that same system.\(^83\) We need to compare it with other fixed-points and with other systems. We need to compare and gather data from different sources and cross-reference it with different information databases, and stay up to date on the possible differences.\(^84\)

Gathering information only from one source is insufficient. For example, a child may draw or paint purple cows. Furthermore, the child may believe that cows are purple. While this may seem nonsensical to an adult, the child may have seen advertisements or cartoons with purple-colored cows.\(^85\) Moreover, the child may never have seen a cow in person. In this scenario, the child used only one source of information, an advertisement or a cartoon, to form the child’s basis for the color of cows. By relying on additional sources; such as zoos, farms, or books; the child may have realized that cows are not purple.

Furthermore, no one questioned whether the “funny-strange” journalist, Borat, was a fake.\(^86\) Borat became famous and many people (including famous politicians, journalists, and often the audience) believed in his actions.\(^87\) Nobody tried to get information from other sources, and nobody checked Borat’s reliability.\(^88\) Everybody just accepted what he said;\(^89\) the information was one-source dependent.

C. “Cincinnati-Hong Kong”—Different Channels

A modern example of information gathering from different channels can be witnessed in an on-line internet call.\(^90\) This scenario involves not only different sources, but different channels as well. For example, Max is skyping with his
friend, Daphne. Daphne is in Hong Kong, Max is in Cincinnati. Max can see and hear Daphne. Max can dial Daphne’s number on his cell-phone at the same time. In front of his eyes, Daphne answers her cell-phone. Max can hear the same ringing tone from his notebook and from his cell phone. The “web camera picture” and the “two voices” are more than double-checking—they are triple-checking. If Max wants to be even more certain that he is talking with his friend, Max could check Daphne’s IP address. At the same time, Max can send his other friend who lives in Hong Kong to visit Daphne. Daphne could open her door for him, and Max from Cincinnati could see both of them through Skype. Additionally, Max could be on-line through a mobile with his friend from Hong Kong, and not only with Daphne. Thus, Max—from abroad—can ensure the place where Daphne is located, Daphne’s identification, and the technological items that belong to Daphne.

D. The Blind Men and the Elephant—Different Methodology

There is a poem based upon an ancient Hindu tale about six blind people who wanted to figure out what an elephant looked like. Each of them had a different image about the “elephant” (e.g., “like a snake,” “like a spear,” or “like a tree”) depending on which part of the elephant they touched (e.g., the trunk, tusk, or knee). The use of more sources (different parts of the elephant) or more channels (six people) to gather information, however, might not produce a more reliable outcome. But with the use of different methods and methodology (seeing, hearing, smelling, weighing, measuring, etc.), the information would be much more precise (than a snake, a spear, or a tree).

E. Triangulation

Triangulation is often used for navigation and surveying. It is based on geometry. Using triangulation, the precise destination of a ship can be established by determining the location of three or more landmarks. The same concept applies to the validation of information. When validating information, “[t]riangulation involves seeking accounts from three or more perspectives.” By checking additional sources, an individual not only corroborates or refutes the

91. See id. (providing free group video calls online); Skyping, URBAN DICTIONARY, http://www.urbandictionary.com/define.php?term=skyping (last visited June 29, 2014) (defining “skyping” as “[u]sing skype to communicate via voice, text message, file transfer and link exchange simultaneously”).
93. Id.
95. Id.
96. Id.
97. Id. at 90.
98. Id.
underlying information, but the individual also increases his or her understanding and knowledge about the topic.  

VIII. DILEMMAS

A. Time and Expenditure

The question always arises: is the cost of prevention lower than any losses incurred without monitoring? If the company assumes that fraud losses would be lower than the cost of prevention, the answer is almost a given. These two points (expenditure and time) may determine the company’s policy, monitoring process, and the depth and multiplicity of any control.

B. Tacit and Direct

The method of information gathering can be tacit or direct. Stronger methods may be noticeable or uncomfortable for the partner-company, which may indicate an element of distrust, which is not a positive indicator. However, the assumption is that anyone who is interested in being taken seriously in the business environment will be happy to build up its reliability and will provide the above-mentioned information for its potential partners. The possible channels can be different. For example, a business can ask the partner company to provide documentation, or make use of registrars, dictionaries, domain searches, webpage information, historical information, statistical office information, local newspapers, or information gained through the chambers of commerce, bar of solicitors, embassies, and department of commerce, etc.

C. Prevention and Proof

The collection of controlled information ensures the reliability of the company—that it exists and performs real business. Additionally, in the case of fraud, this information will work as an aid in conducting the investigation (more ties, more evidence, and a better and faster process). For instance, if you take a photo of the management of the company, it is only one piece of prevention; however, this photo may also help identify and find criminals later on.

99. Id.
100. See, e.g., Kathleen M. Sarver, Analytical Data Validation - It’s Worth the Cost (Part 2 of 2), COX-COLVIN & ASSOC., INC. ENVTL. SERV., http://www.coxcolvin.com/Analytical_Data_Validation_Benefits.php (last visited Apr. 18, 2014) (Although data validation is time-consuming and expensive, in the environmental field, the benefits of data validation outweigh the cost).
101. See Darby, supra note 24 (providing ways to validate whether a company is legitimate).
102. See id.
103. See id.
D. The Traffic Is Not Responsible for Traffic Accidents

Analogically, neither globalization, technical development, nor the information channels-based businesses are evil. They are simply neutral. For example, road traffic is regulated and naturalized. Likewise, the culture of information channels-based business will be naturalized. If the whole ocean is muddied, let us first clean the water around us, to see what is going on, and what can affect us. If we cannot organize the system as a whole, then we will need to create our own small, secure-areas, and/or be more critical and circumspect in our business interactions.

IX. TRAIN OF THOUGHT—HOW DOES CHECKING WORK?

How can we check the seat of a company for example? The train of thought is as follows: if a company was moved and/or established somewhere in a city in 1982, we may be able to find a headline about this event in a local newspaper at this location in that time (realistically nobody will go back and change historical records). For example, we may gather information in the following ways: the “seat of a company” is a fixed-point in a theoretical meaning because each postal mail can be delivered worldwide just into one location—each address has just one mailing address. Thus, if a businessperson compares the results of the location searches acquired by different methods and channels, the data reliability will increase. We can deliver documents using a recorded delivery service for testing purposes—is the same address provided by the domain name service as by the seat provided by business registry? Does the acquired location match with entitlement of the usage of the immovable estate address? Is it the same location as the IP address or DNS search suggests?

A local lawyer and notary may visit the place physically, as well (Cincinnati-Hong Kong). Check the location on an independent interactive on-line map as well. Can we find the same address in the Yellow Pages, office registrars, or on webpages? Can the business registry, chamber of commerce, ministry of commerce, in-house lawyer, a local lawyer, and/or a notary mandated by us confirm the same company seat? And what about a personal visit? Step-by-step, every fixed-point checked by different channels and methods will increase the trustworthiness of the seat of our new partner company, and the matches in data from different sources decreases the fraud risk.

The general aim is simple: Stay aware. Stay sceptical. Stay critical. Follow the logic of the simulations. Do your own private investigations. If you notice discrepancies among gathered data, it could mean something strange and should raise a red flag. Without adequate knowledge, we cannot make an informed

104. See PIERCE, supra note 94, at 83 (“Reliable data is dependable, trustworthy, unfailing, sure, authentic, genuine, reputable. Consistency is the main measure of reliability.”).
105. See infra Part VII, C.
106. See PIERCE, supra note 94, at 83.
decision—just unconditionally accept, in an environment where accepting means losing.

X. APPENDIX

The following are tips for the businessperson on how to get information about a company. At all times one should compare the results and match the fixed-points with each other:

- Gather registry information about the company. Check the chambers of commerce; get the data from the online database of the official registry (if the actual country does not have online registrars, mandate a lawyer in that country to get it and deliver to you the official transcripts); contact the tax authorities and gather official information; order a copy of the certificate from the registry.

- Check the scope of businesses (approved activity list from the registry court); certificate about registration or an incorporating document; get data about the equity of the company, corporate property and deed of association (and its date); check the electronic signature, and check the electronic signature provider company; contact the mentioned partner companies and/or memberships. Obtain a copy of power of procuration, information of holders of procuration (name and address), information of kind of procuration (single or common, general or limited to specified areas).

- Check the Internet Protocol (“IP”) address\textsuperscript{107} and the Domain Name System (“DNS”)\textsuperscript{108} of the partner company. Gather data through DNS portals or Whois services\textsuperscript{109} which contain full information package: company name and address country, domain creation date (which can be interesting as well), registration, and expiry date. Is the domain registered in the same country where the company is seated? If not, why?

\textsuperscript{107} Marshall Brain & Stephanie Crawford, \textit{How Domain Name Servers Work}, HOWSTUFFWORKS.COM, http://computer.howstuffworks.com/dns.htm (last visited April 19, 2014) (explaining that an IP address is the unique identifier of a particular machine connected to a network).

\textsuperscript{108} Id. ("DNS is a protocol within the set of standards for how computers exchange data on the Internet and on many private networks, known as the TCP/IP protocol suite. Its basic job is to turn a user-friendly domain name like “howstuffworks.com” into an Internet Protocol (IP) address like 70.42.251.42 that computers use to identify each other on the network.").

\textsuperscript{109} Ian J. Block, \textit{Hidden Whois and Infringing Domain Names: Making the Case for Registrar Liability}, 2008 U. CHI. LEGAL F. 431, 431 (2008) ("When registering domain names for websites, registrants must supply contact information that appears in the Whois database. The Internet Corporation for Assigned Names and Numbers (‘ICANN’) maintains the Whois database as a means of making information available about website owners (registrants), so that disputes concerning those sites can be resolved quickly.").
Check the name of the administrator (address, phone, fax, e-mail). Check the history of the domain (does it have a controversial history?); check the second-selling domain-market, whether the domain is on the sell-list or not.

- Check the history of the company. Check the financial data, stock markets, statistics, on-line newspaper, local newspapers, advertising, consumer and company feedbacks. Check online and paper-based black debt list, bankruptcy, liquidation, cancellation, execution lists (pay attention to abbreviations, regarding the above mentioned)—is there a law suit against the company, what is the subject of the case? Get information about the tax-number, bank account, statistical identification number and compare them with what you have gathered via other methods and channels; check different registrars and dictionaries; if you need permission, apply for these documents or ask the partner company to forward them; get official account statements from the company about its utility account balance (that can be public information), ensure that the bank account belongs to the company; search for management changes.

- Check client and company references, including online feedback. Check the identity of comment and feedback providers, check the extra-links on the website—are they real comments or not? Find people or companies who have had any contacts or deals in the past with your new partner company.

- Check the company’s physical addresses. Send a certified delivery, check the phone numbers and fax numbers, check the different “contact and mailing addresses”; ask different questions through different channels—can they be reached via any of these? Find the address of the company on an online map (street view) and in different registrars, etc.

- Obtain information about managers, auditors, executive employees and officers, confidential clerks, and members of the board of supervision, including their names and addresses. Get information about them from the partner company and from the registry; check the financial situation of the partners; check the “Politically exposed person” (“PEP”) risk; get

110. Louis de Koker, The 2012 Revised FATF Recommendations: Assessing and Mitigating Mobile Money Integrity Risks Within the New Standards Framework, 8 WASH. J.L. TECH. & ARTS 165, 174 n.17 (2013) (“Politically exposed persons (PEPs) are generally defined as people who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, or important political party officials. PEPs, their family members, and close business associates may pose a corruption risk.”).
information whether they have ever been arrested, and if yes, for what crime. Were they a member of a cancelled or a liquidated company (in the past); were they disqualified or wanted persons? Find information in the local newspaper about the company and about the members from the time when the company was established; search for information about the members of the company in official and non-official registrars, online social networks, institution registrars, etc. Record phone calls, videoconferences, take “friendly meeting photos” and videos about managers during the personal visit. Conduct a social portal and career portal search; check the name of the representatives through internet search engines. Check the representatives of the company in registrars, are they persona non grata, disqualified or wanted?

- Obtain information about the agents of the company. Obtain a copy of the agency agreement (power of agency, trade agency and representation). Get information about the name and residence of representatives; the date of establishment of the agency agreements; duration, and terms of the power of agency of the representatives and agency persons; and get a copy of the power of authorization (where the signatures of the management are given). Mandate a public notary who may justify the signature and identity of the manager.

- Obtain information about the solicitors and legal counsels of the company. Contact the company lawyers. Check the mandate of the legal counsel and the representatives in the court register. Get information from the company’s lawyer and solicitor bar about the company lawyer regarding his/her bar association, registration, and about his/her past.

- A possible long-term solution could be to build a profile based on the experience of ex-business partners; the members of the group (and affiliates) could use it as a “feedback database system.” The finance, controlling, and/or legal department may adopt internal policies regarding data gathering.

- Repeat all these processes from time to time, or at least before new major actions as trustworthy companies may go rogue over time, or proprietary circumstances and personnel may also change.
MODERN DEVELOPMENTS IN WHITE-COLLAR CRIME

R. Samuel Gilley*

In the legal community, experience is imperative. But why? Native wit suggests that this is so because the issues lawyers face – whether legal or professional, practical or technical – are myriad and ever-changing, such that no amount of education could provide a young attorney with the answers they need to find immediate success in the legal market. Recognizing this reality, law school administrators (who are no fools, by the way) have shifted some educational emphasis from doctrinal coursework to internships, externships and summer clerkships. And it is in those outside-the-classroom situations that students get begin to get a feel for which issues, legal and otherwise, matter most to lawyers.

But fundamental to a legal education is the intellectual environment law school curricula submerge their students in on a day-to-day basis. (Most) law students spend countless hours playing mental racquetball – the Socratic method – with professors whom are experts in their fields and some of the most talented lecturers that higher education has to offer. And these professors have not only mastered doctrinal law, but, as scholars of the law, they stay abreast of new developments in their areas of expertise. This knowledge is of immeasurable importance to law students from an information-cost standpoint because most practitioners are too busy maintaining their practices to “keep up” on every change in their field. Thus, when a professor funnels it to the students whom are diligent enough to understand it inside and out, these students become increasingly valuable to the otherwise-overwhelmed practicing attorneys. There are countless anecdotes of first-year attorneys contributing up-to-date skills and knowledge to established attorneys’ practices – in one notable example, a fellow federal clerk was familiar enough with the evolution of insider trading litigation that his supervising attorney took on a relevant case that would have otherwise been outside of his expertise, let alone his comfort zone.

Over the last several years, my education inside and outside the classroom has left me aspiring to litigate in federal court with an eye toward white-collar crime. So, given the creative freedom that I have with this paper, I decided to combine my practical and intellectual educational experiences, as described

* Law clerk to the Honorable Charles R. Simpson III, United States District Court, Western District of Kentucky. 2014 graduate of Salmon P. Chase College of Law.
2. Chase recently broke ground on this front by creating its “semester in practice” program. In that program, students can spend an entire semester working in an approved legal position and earn a semester’s worth of credit. See http://chaselaw.nku.edu/students/registrar/course-catalog/semesterinpractice.html.
above, to research and write about modern developments in the white-collar criminal landscape. Then my next question became: what developments should I write about? This is where my time clerking for a former Assistant United States Attorney (“AUSA”) turned prominent white-collar criminal defense attorney and, currently, for a federal judge helped key me in on what areas of a white-collar criminal practice are most important. I will refer to this attorney as Bob.

What stands at the forefront of how I now perceive the practice of white-collar criminal law is what I refer to as “productive cooperation.” In my time working with Bob, I promptly recognized that, much like the first forty-eight hours in the search for any kidnap victim, the first steps that the subject of a federal investigation takes are often the most critical – especially where 97% of federal crimes that were prosecuted to conclusion in 2012 did not go to trial.\(^3\) And in my opinion, these first steps can be broken down into three categories: pre-arrest questioning, post-arrest cooperation, and post-indictment asset forfeiture. A calculated approach to these steps evinces an appreciation that any misstep during them could mean the difference between maximum-security federal prison, a verdict of not guilty, or an AUSA’s decision not to bring charges. Such an appreciation is, in other words, absolutely essential.

First, regarding pre-arrest activities, I discovered that a suspect’s behavior during police questioning and his having an “eager to help” appearance can make or break his chances of freedom. Then, during the post-arrest/charge stage, I have seen how a suspect’s willingness and ability to cooperate by providing useful information set the tone for how the prosecution will charge the suspect or influence the suspect’s sentencing – two priorities of any criminal defendant. And, lastly, in the event that the suspect is indicted on charges involving money laundering – as white-collar charges most frequently do\(^4\) – I witnessed first-hand how significantly asset forfeiture can affect the defendant and, more importantly, his ability to retain counsel.

Thus it is these three arenas – pre-arrest questioning, post-arrest cooperation, and post-indictment asset forfeiture – that my experience has shown to be of utmost importance to white-collar crime practice. Ironically, these are not areas of the law practice that a layperson would think of as traditionally legal. Nevertheless, it is within these three arenas that I have researched and examined recent legal developments of pertinent import. This paper will discuss my findings.\(^5\)

To that end, Part I will discuss the recent Supreme Court decision in *Salinas v. Texas* - a decision regarding prosecutors’ ability to use suspects’ pre-arrest

---


5. For confidentiality purposes, I will use fictitious names and scenarios in all of my anecdotes.
silence against them at trial - and the implications it may have on criminal investigations and prosecutions. Part II will discuss the Department of Justice (“DOJ”) and other regulatory agencies’ increasing emphasis on eliciting cooperation from criminal suspects, how the value of such cooperation is currently evaluated, and AUSAs’ admitted ability to detect cooperators’ untruthfulness. Lastly, Part III will discuss the Supreme Court case Kaley v. United States⁶ – a case involving criminal defendants’ rights to challenge probable cause supporting judicially imposed asset forfeiture in an adversarial hearing – and its potential implications within the Sixth Circuit.

I begin each section with a hypothetical legal obstacle, if you will, then use that hypothetical to highlight and facilitate my discussion in that section. Through this discussion, I hope to inform the reader of these modern developments, emphasize their importance and, selfishly, arm myself with a body of knowledge so relevant to white-collar criminal law practice that I could be of immediate value to any entity practicing law in that realm. Do enjoy.

I. PRE-ARREST SILENCE AND THE FIFTH AMENDMENT

It is February 2013 and, because you are a Certified Public Accountant (“CPA”), you agree to prepare and file your dimwitted and financially troubled brother’s 2012 tax return. In doing so, and upon your brother’s direction, you note substantial deductions for charitable donations that your brother claims to have made in 2012. Unfortunately, whether you knew it or not, your brother has never donated to a charity in his life.

Several months later, your brother receives a notice from the IRS explaining the deficiency and requesting that your brother concede liability for the unsubstantiated deductions. You, on the other hand, receive a call from the DOJ, who asks you to come into their local office to answer a few questions and “clear your name” of any criminal liability for tax fraud. Overcome with fear, you reluctantly oblige.

When you meet with a DOJ agent, the agent’s questions hurriedly take a hostile turn. The agent does not read you your Miranda rights because you are not under arrest or in police custody and your meeting is “voluntary.” He asks you preliminary questions about your relationship to the taxpayer – your brother – and has you verify that you signed the return as a tax return preparer. He then, blatantly skeptical of your competence as a CPA, questions your qualifications as a preparer. He asks you if you knew that your brother had been in financial trouble, to which you hastily reply “yes.”

Then the agent asks you if knew that your brother had not made the charitable donations that you claimed deductions for on his tax return. Recognizing that an answer would either incriminate yourself or your brother, you remain silent. Manifestly agitated, the agent asks you two more times, “did

---

you know your brother hadn’t made these donations in 2012?’’ You remain silent and eventually ask if you can speak to an attorney. The agent says that is fine and informs you that because you are not under arrest or in custody, you are free to leave at any time. You leave without hesitation, confident that you did not say anything that could hurt you or your brother if the DOJ chooses to initiate criminal proceedings. Your silence, however, may have said enough.

In light of the Supreme Court’s recent decision in Salinas v. Texas, your silence in response to that question could be used against you in a subsequent prosecution – here, probably a prosecution for willful disclosure of false documentation to the IRS under 26 U.S.C. § 7207. Under the facts of this case, however, the DOJ would probably need more evidence than the tax preparer’s silence to successfully convict him under 26 U.S.C. § 7207. But in many cases, like in Salinas, a defendant’s silence in response to an incriminating question may be the final piece of circumstantial evidence that convinces a jury to convict him or her of the charges at hand.

A. Salinas v. Texas

In Salinas, two brothers were shot and killed in their Houston home, at which the petitioner, Genovevo Salinas, had attended a party the night before. There were no witnesses to the shooting, but a neighbor heard the gunshots and saw a dark-colored vehicle speed away. The investigation led police to Salinas, who had a dark blue vehicle parked in his driveway. Police asked Salinas to accompany them to the station for question and hand over his shotgun to “clear his name,” and he voluntarily complied.

Salinas’s interview lasted approximately one hour and was noncustodial. Police never read him Miranda warnings. He answered all of the officer’s questions during the interview until he was asked whether his shotgun “would match the shells recovered at the scene of the murder.” To that question, Salinas declined to answer and nervously “[l]ooked down at the floor, shuffled his feet, bit his bottom lip, clenched his hands in his lap, [and] began to tighten up.” Petitioner was not charged, however, until a man came forward several days later and told police that he heard Salinas confess to the killings.

8. Id. at 2184.
9. Id. at 2178.
10. Id.
11. Id.
12. Id.
15. Id.
16. The trial was not held for twelve years because police were unable to locate the suspect.

Id.
At trial, Salinas refused to testify and objected to the prosecution’s use of silence and nervous reaction during the police interview.\textsuperscript{17} He argued that use of his silence violated his Fifth Amendment privilege against self-incrimination, but the trial court disagreed. On appeal, the Texas Court of Appeals also rejected Salinas’s arguments, explaining that pre-arrest, pre-\textit{Miranda} silence is not “compelled” within the meaning of the Fifth Amendment.\textsuperscript{18} The Texas Court of Criminal Appeals affirmed, and the Supreme Court granted certiorari to answer “whether the prosecution may use a defendant’s assertion of the privilege against self-incrimination during a noncustodial police interview as part of its case in chief.”\textsuperscript{19}

In a 5-4 decision, the Supreme Court held that in order for Salinas to rely on the privilege against self-incrimination in a non-custodial, pre-\textit{Miranda} interview, he must have expressly invoked the privilege.\textsuperscript{20} Accordingly, so long as police do not deprive such an interviewee of the ability to voluntarily invoke the privilege via coercion or otherwise, the interviewee’s silence will not suffice to trigger the privilege.\textsuperscript{21} Oddly, and as several concurring justices were quick to point out, this holding does not answer the question presented – if Salinas did invoke the privilege, could the prosecution use it at trial?\textsuperscript{22} But even as such, this holding will have serious implications for criminal defendants and prosecutors.

The Court supported the holding by first reiterating its long-standing principle that “[t]he privilege against self-incrimination ‘is an exception to the general principle that the government has the right to everyone’s testimony.’”\textsuperscript{23} Thus to prevent the privilege from shielding information not properly within its scope, it reasoned, a witness seeking protection of the privilege must claim it and put the government on notice.\textsuperscript{24} This notice then gives the government an opportunity to argue that the testimony it seeks will not be self-incriminating or, if the testimony will be self-incriminatory, cure any risk by granting immunity.\textsuperscript{25}

There are, however, two exceptions to the express invocation requirement. Yet neither applies in the context of noncustodial, voluntary interviews. The first, that a criminal defendant need not take the stand and assert the privilege at his own trial,\textsuperscript{26} is patently inapplicable in this context. The second applies when defendant’s failure to invoke the privilege is excused where his failure is a result

\textsuperscript{17} Id.
\textsuperscript{19} Salinas v. Texas, 133 S. Ct. 2174, 2178 (2013).
\textsuperscript{20} Id. at 2184.
\textsuperscript{21} Id.
\textsuperscript{22} Salinas v. Texas, 133 S. Ct. 2174, 2184 (2013) (Thomas, J., concurring in judgment).
\textsuperscript{23} Salinas, 133 S.Ct. at 2179 (citing Garner v. United States, 424 U.S. 648, 658, n. 11 (1976)).
\textsuperscript{24} Id. (citing Minnesota v. Murphy, 465 U.S. 420, 425, 427 (1984)).
\textsuperscript{25} Id. (citing Hoffman v. United States, 341 U.S. 479, 486 (1951)); Kastigar v. United States, 406 U.S. 441, 448 (1972).
\textsuperscript{26} Griffin v. California, 380 U.S. 609, 613–615 (1965).
of governmental coercion and is, therefore, involuntary.\textsuperscript{27} Courts uniformly apply this exception when a suspect has not been \textit{Mirandized} and faces the “inherently compelling pressures” of a custodial interrogation, which is plainly not at issue.\textsuperscript{28}

But the defendant at issue was not in a custodial interrogation; nor can it be said that the circumstances surrounding the interview created a coercive environment that rendered his failure to invoke involuntary.\textsuperscript{29} In fact, Salinas agreed to accompany the officers to the station and was told that he “was free to leave at any time during the interview.”\textsuperscript{30} So the silence at question does not fit the requirements of either existing exception. The Court refused Salinas’s invitation to create a third exception for cases where a noncustodial witness refuses to give an answer that police suspect would be incriminating.\textsuperscript{31} It did so because, under \textit{Roberts v. United States}, a defendant does not invoke the privilege by remaining silent, \textsuperscript{32} and under \textit{Minnesota v. Murphy}, the express invocation requirement applies even when police suspect that the answer would incriminate the witness.\textsuperscript{33}

The Court ended its opinion convincingly by reminding us that “the Fifth Amendment guarantees that no one may be ‘compelled in any criminal case to be a witness against himself’; it does not establish an unqualified ‘right to remain silent.’”\textsuperscript{34} And so it stands, that a suspect in a noncustodial, pre-\textit{Miranda} interview can only invoke the Fifth Amendment privilege against self-incrimination by saying that he is doing so.

\textbf{B. Salinas and Potential Prosecutorial Abuse}

From a prosecutorial standpoint, this decision can be considered a general win. In essence, the Supreme Court has opened the door for police to use “hide the cards” tactics in interviewing potential suspects – for example, asking a suspect to come “clear their name,” like in \textit{Salinas}, or simply telling the suspect that they are not being investigated. After the suspect agrees to the interview, police are free to ask him incriminating questions, and, now, either his incriminating response or silence can be used against him at trial – a remarkable catch-22.\textsuperscript{35} This can be another powerful tool in the tool belt of prosecutors and their law enforcement arms. But, especially in the white-collar context,

\begin{itemize}
\item \textsuperscript{27} Salinas v. Texas, 133 S. Ct. 2174, 2180 (2013).
\item \textsuperscript{28} See Miranda v. Arizona, 384 U.S. 436, 467-68, n. 37 (1966).
\item \textsuperscript{29} Salinas, 133 S.Ct. at 2180.
\item \textsuperscript{30} Id. (quoting Brief for Petitioner 2-3).
\item \textsuperscript{31} Id. at 2181.
\item \textsuperscript{32} 445 U.S. 552, 560 (1980).
\item \textsuperscript{34} Salinas v. Texas, 133 S. Ct. 2174, 2182-83 (2013).
\item \textsuperscript{35} There is, technically, a third option: lying. But white-collar lawyers should inform their clients of the potential penalties under 18 U.S.C. § 1001 (2012), the false statements statute.
\end{itemize}
individuals who are aware of Salinas may actually be less eager to voluntarily interview with law enforcement.

White-collar criminals are, generally speaking, more affluent and better educated than common criminals.\(^{36}\) With that affluence, white-collar criminals are more likely to permanently retain counsel, or “have a lawyer”;\(^{37}\) with more education, white-collar criminals are also likely to be more careful and/or hesitant in dealing with police. Any competent attorney retained by white-collar clients will tell the client to call them immediately after “they bec[o]me aware that they might be the subject or target of an investigation.”\(^{38}\) And cognizant of Salinas and the federal false statements and obstruction of justice statutes (both statutes carrying terribly harsh penalties),\(^{39}\) these attorneys will tell their clients not to speak with law enforcement alone.\(^{40}\) Thus, once Salinas becomes common knowledge in the white-collar legal community, law enforcement may actually find witnesses and suspects less likely to cooperate before any arrests are made in an investigation.

In sum, it is more than arguable that criminal defendants will see a decrease in constitutional protections resulting from Salinas. But this is most likely to affect common criminals who are not well-versed in the law. And while white-collar criminals are better equipped to avoid a situation like that in Salinas, a reckless client can still walk into the trap this holding will allow law enforcement to lay.

II. COOPERATION AND SUBSTANTIAL ASSISTANCE

One of your clients, Joe Businessman, comes to your office and reports his belief that the DOJ is going to bring charges against him for participating in a “ponzi scheme.” He readily admits that he and Joe Trader, his business partner, have been soliciting investors to invest in CincyFund, which they had pitched as a lucrative way to make money in “day trading.” Joe Businessman’s major role in the scheme was recruiting investors, while Joe Trader both recruited and held himself out as CincyFund’s experienced investment advisor. Businessman and Trader told investors they would purchase large blocks of stocks in overseas markets and liquidate them into cash prior to market close, generating above-market earnings of 10 to 15%. Despite these representations, however,

---

CincyFund was not a legitimate business and had never traded a stock or invested on behalf of investors.

Over seven years, CincyFund defrauded investors of over $8.9 million. As new investors poured money into the apparently successful fund, Trader and Businessman used that money to pay off earlier investors in class, ponzi-scheme fashion. But after seven years of lavish personal spending and extensive fraud, the new investments could not keep up with Trader and Businessman’s spending, and the scheme collapsed. This caught the eye of federal regulators who launched an investigation while Trader and Businessman continued on their path of destruction. During the investigation, they lied to law enforcement, continued to solicit money, and created false account statements and promissory notes to make CincyFund seem legitimate. CityFund’s only account, however, had a balance of $995.88 – a fact that investigators quickly discerned. There is no doubt in your mind that Joe Businessman is going to prison.

Yet, despite Businessman’s unconscionable, insidious behavior and an applicable sentencing range of 97-121 months for mail fraud, wire fraud, obstruction of justice, and tax evasion, the court only sentences him to 65 months in prison – a difference of almost five (5) years. The court sentenced Trader, on the other hand, to 131 months in prison. So how did your client receive such a lenient sentence? He cooperated. And, yes, the facts I used in this anecdote, other than the fictitious names, are all real. They are based on a case that appeared before the Honorable Herman J. Weber, Senior District Court Judge for the Southern District of Ohio in 2013.

But what kind of cooperation could save a defendant five (5) years in prison?

In United States v. Snelling, the case on which this anecdote is based, the United States Attorney’s Office (“USAO”) for the Southern District of Ohio recommended that Judge Weber depart from an applicable range of 97-121 and sentence Jerry Smith (known above as Joe Businessman) to 72 months for his “substantial assistance in the investigation and prosecution of others.” The Court was ultimately persuaded by the USAO, among other considerations, and sentenced Jerry smith to 65 months in prison. As surprising as this reduction was, it happens all the time. In fact, a similar example existed when Worldcom’s former CFO, Scott Sullivan – arguably the architect of the accounting fraud – cooperated against Worldcom’s CEO, Bernard Ebbers, and received a sentence...

41. The number of charges brought are slight in comparison the crimes actually committed. For example, see 18 U.S.C. § 1519 (anticipatory obstruction of justice) and 18 U.S.C. § 1348 (securities fraud).
44. Watkins, supra note 43.
of just five (5) years, while Ebbers received a sentence almost five times as long.\textsuperscript{45} The value of cooperation is evident. But how is it so important? Over the past decade, cooperation has become a priority of federal prosecutors\textsuperscript{46} and, as of recent, regulatory agencies – specifically, the Securities and Exchange Commission (“SEC”).\textsuperscript{47} The SEC, an entity without criminal prosecutorial authority, has even gone so far as to render offenders who assist their investigations eligible for reduced criminal penalties.\textsuperscript{48} And because the SEC or the DOJ investigates most white-collar crimes, cooperation may be particularly important in this context. Moreover, this dramatic shift-in-emphasis\textsuperscript{49} was undoubtedly brought on, at least in part, by the Enron-induced realization that prosecuting complex financial crimes is terribly difficult.\textsuperscript{50} The statistics displaying increased cooperation are especially eye-opening in the Sixth Circuit and the Southern District of Ohio, making cooperation even more important to someone interested in white-collar crime and pining for a position as an AUSA in that exact district – i.e. myself.

In the Southern District of Ohio, 26.6\% of criminals that were sentenced in 2012 received a Substantial Assistance Departure under §5K1.1 of the United States Sentencing Commission’s Guidelines Manual, compared to only 11.7\% nationally.\textsuperscript{51} The Sixth Circuit granted §5K1.1 departures in 21.2\% of sentences.\textsuperscript{52} Like with Joe Businessman, substantial assistance or §5K1.1 departures are given upon recommendation by a USAO. Thus the defendant’s relationship and interactions with the AUSA at hand are critical to his efforts to obtain a lenient sentence, and substantial assistance departures are the primary route for achieving that. To fully understand how cooperation in the context of substantial assistance works, the following will discuss: 1. when defendants can obtain a substantial assistance recommendation; 2. the procedure AUSAs follow.

\textsuperscript{47} SEC Release No. 34-61340 (Policy Statement Concerning Cooperation by Individuals in its Investigations and Related Enforcement Actions). See also Press Release, U.S. Sec. & Exch. Comm’n, SEC Announces Initiative to Encourage Individuals and Companies to Cooperate and Assist in Investigations (Jan 13, 2010) (available at http://www.sec.gov/new/press/2010/2010-6.htm). In the latter release, the SEC’s Enforcement Division Chief announced the Division’s plan to ramp up investigations by relying on cooperators. For purposes of brevity, however, this article will focus on the USAOs’ procedure for issuing substantial assistance recommendations.
\textsuperscript{48} Press Release, supra note 48.
\textsuperscript{49} See generally Baer, supra note 46.
\textsuperscript{51} USSC, Sourcebook of Federal Sentencing Statistics, OHIO, Southern (Fiscal Year 2012).
\textsuperscript{52} USSC, Sourcebook of Federal Sentencing Statistics, tbl. N-6 (Fiscal Year 2012).
in determining whether to give a substantial assistance recommendation; and 3. how AUSAs can be deceived by cooperators in making that determination.

A. Proffer Sessions: “Queen for a Day”

Because the Sentencing Guidelines now vest prosecutors with complete authority to hand out rewards for assistance, prospective defendants must cooperate and negotiate with prosecutors if they have any hopes of a reduced sentence. A defendant’s only means of gaining such aid is by “proffering” to a federal prosecutor – that is, he must volunteer the information that he will provide in exchange for leniency – under a proffer or “Queen for a Day” agreement. This agreement covers the terms of the defendant’s initial offer of information, known as a “proffer session”, which ordinarily occurs before any cooperation agreement is reached. A proffer session is critical for defendants because it is the “conventional first step” in the process where defense counsel provides information to the government in an attempt to establish credibility and convince the government to consider a cooperation, plea, or non-prosecution agreement.

In a typical proffer session, an AUSA, defense counsel, the defendant, and often a representative of the investigative agency involved in your case (i.e. FBI, ATF, IRS Criminal Division, etc.) will meet in a “proffer room” – nothing more than walls, a desk, and a few chairs – to discuss the kinds of assistance the defendant may be able to render. The AUSA gives the defendant the proffer agreement at the outset, which states that he is not yet officially cooperating. The agreement also explains that, unless the defendant attempts to deny anything he said in the meeting at trial, his statements will not be used against him. Absent such an agreement, nothing the defendant said in an attempt to cooperate would be admissible in any criminal proceeding under Fed. R. Evid. 410 and Fed. R. Crim. P 11(f). And although these rights are well-settled, the Supreme

---

54. Id.
55. Id. at 5. In a proffer session, the individual will either be considered a target or a subject. This article focuses on the proffer sessions and targets, the more typical scenario. If the individual is a subject, however, this means that the law enforcement agency is unsure about your status or involvement. What a subject says in during proffer session can turn him or her into a witness or a target. For more, see generally http://whitecollarcrimenews.com/2010/01/03/what-is-a-proffer-session-and-what-should-you-do/.
57. Gershman, supra note 56, at 6.
58. Id.
Court’s decision in United States v. Mezzanatto now allows defendants to waive their protections through the proffer agreement.

After a defendant reads and signs the proffer agreement, the AUSA will explain that the defendant has no obligation to speak with him. He is likely to add that the defendant can confer with defense counsel in private at any time. Then, after emphasizing that truth is the most important consideration, the AUSA will commence the interview. During this first interview, the AUSA will know the answer to almost every question that he or she asks. This is an opportunity for the AUSA to gauge the defendant’s truthfulness and usefulness. A good defense attorney, however, will never bring a defendant to a proffer session unless he or she knows that their client will be truthful. And even then, the truth can only get a defendant so far.

Once the government determines that a defendant is truthful, it will need to see that the defendant can provide information that it can use in the prosecution of others. Generally speaking, it will (read: should) attempt to corroborate any information that the defendant provides. And if the AUSA or enforcement agents like what he has to say, they may propose a cooperation agreement request another proffer session. More often than not, the prosecution will offer a substantial assistance letter to induce a cooperation agreement.

B. Substantial Assistance Departures

Under the permissive United States Sentencing Guidelines (“USSG”), sentencing courts are presented with a “guideline range” – calculated for each defendant based upon offense seriousness, criminal history, level of participation, age, acceptance of responsibility, etc. – that they must consult when sentencing a convicted defendant. But an AUSA may file a motion with that court recommending that it depart from the applicable guideline range on the basis that the defendant provided “substantial assistance in the investigation or prosecution of another.” In many cases, this allows a court to depart below otherwise-mandatory minimum sentences. Because this authority is granted pursuant to

61. Naftalis, supra note 54, at 17.
62. Zapp, supra note 58.
63. Id.
64. Id.
65. Id.
66. See section II.B.
69. See generally U.S. SENTENCING COMMISSION, FEDERAL SENTENCING GUIDELINES MANUAL (2013) [hereinafter USSG].
70. Id. at § 5K1.1.
USSG § 5K1.1, these motions are generally referred to as 5K1.1 or substantial assistance letters. The United States Attorneys’ Manual (“USAM”) lays out the considerations and procedures that AUSAs must weigh and follow in filing such a motion. The USSG instructs courts to accept such a recommendation upon finding certain factors. I will examine each in turn.

The USAM dictates the circumstances under which it is appropriate for an AUSA file a motion pursuant to USSG § 5K1.1. Under USAM 9-27.400, an AUSA can enter into a plea agreement with a defendant that binds the AUSA to “[m]ake a recommendation . . . for a particular sentence, with the understanding that such recommendation or request is not binding upon the court.” However, such a recommendation must be approved by the United States Attorney, the Chief Assistant United States Attorney, and supervisory criminal Assistant United States Attorneys. And the AUSA must maintain documentation of the facts behind the justification for each substantial assistance motion.

Although it is not always so in practice, a prudent AUSA determining whether to agree to such a plea is instructed to weigh:

1. The defendant’s willingness to cooperate in the investigation or prosecution of others; 2. The defendant’s history with respect to the criminal activity; 3. The nature and seriousness of the offense or offenses charged; 4. The defendant’s remorse or contrition and his/her willingness to assume responsibility for his/her conduct; 5. The desirability of a prompt and certain disposition of the case; 6. The likelihood of obtaining a conviction at trial; 7. The probable effect on witnesses; 8. The probable sentence or other consequences if the defendant is convicted; 9. The public interest in having the case tried rather than disposed of by guilty plea; 10. The expense of trial and appeal; 11. The need to avoid delay in the disposition of other pending cases; and 12. The effect upon the victim’s right to restitution. Moreover, when filing the 5K1.1 motion, the AUSA should consider the timeliness of the cooperation, the results of the cooperation, and the nature and extent of the cooperation when compared to other defendants in the same or similar cases in that district. But even if the AUSA weights these facts and

73. See generally U.S. Attorney’s Manual 9-27.00 [hereinafter USAM].
74. USSG, supra note 70, at § 5k1.1
75. USAM, supra note 74, at 9-27-730.
76. Id. at 9-27-400(B).
77. Id.
78. Id.
79. See section III.
80. USAM, supra note 74, at 9-27.420(A).
81. Id. at 9-27.730.
decides to go through with the motion, the recommended sentencing departure is not guaranteed.

Sentencing courts determine appropriate sentence reductions have full authority to deny any 5K1.1 motions.\(^{82}\) Under USSG §5K1.1, a sentencing court must determine whether a defendant’s assistance is deserving of the recommended departure based upon the following factors: 1. The court’s evaluation of the significant and usefulness of the defendant’s assistance, taking into consideration the government’s evaluation of the assistance rendered; 2. The truthfulness, completeness, and reliability of any information or testimony provided by the defendant; 3. The nature and extent of the defendant’s assistance; 4. Any injury suffered, or any danger or risk of injury to the defendant or his family resulting from his assistance; and 5. The timeliness of the defendant’s assistance.\(^{83}\) In practice, however, courts rarely deny the AUSA’s 5K1.1 motion.\(^{84}\)

Accordingly, although AUSAs’ definitions of “substantial assistance” may vary from district to district (a topic beyond the scope of this article), each individual AUSA has immense, and, perhaps, unchecked, discretion in determining whether a defendant’s cooperation is worthy of a 5K1.1 letter. And because the USAM is advisory in that regard, it will be helpful to determine what factors AUSAs really consider in evaluating a defendant’s cooperation.

C. “Cooperation is all about perception shaped by personality”

There has been little, if any, study of the cooperation process and cooperation agreements in the federal context.\(^{85}\) Many suggest that this a product of a process that is inherently difficult to analyze,\(^{86}\) because there are varying standards between districts and attorneys,\(^{87}\) or the result of tacit agreement between prosecutors and defense lawyers that the cooperation system should be kept out of the public eye.\(^{88}\) Recognizing the need for such a study, one legal scholar, Professor Ellen Yaroshefsky, used her resources and connections to interview twenty-five former AUSAs and sixteen defense attorneys who had practiced in federal courts in hopes of shedding light on the process. In doing so, she sought out to answer the following questions: 1. The extent to which AUSAs believe that they are able to obtain truthful information from cooperators and the basis

\(^{82}\) Gyurci, supra note 73, at 1260.

\(^{83}\) USSG, supra note 70, at §5K1.1.

\(^{84}\) Gyurci, supra note 73, at 1261.

\(^{85}\) Yaroshefsky, supra note 72, at 919.

\(^{86}\) Id.


\(^{88}\) Id. (quoting Harvey A. Silvergate & Andrew Good, It Didn’t Start With Ken Starr: Starr Teaches, REASON at 26-28 (1999)).
for those beliefs; 2. The safeguards and techniques utilized to assure the truthfulness of cooperators; and 3. Perceived problems with obtaining truthful information from cooperators. The following will discuss and summarize her most compelling findings.

The former AUSAs were quick to acknowledge that mandatory minimum sentencing incentivizes cooperators to lie. Even defense attorneys, one explained, are desperate to get their clients a 5K1.1 letter because they are often the only way for the client to escape a frequently harsh mandatory minimums and hypercriminalization. And despite this awareness, most of the former AUSAs acknowledged that “[y]ou never really know if a person has told the truth” or “the extent of a lie until you start preparing for trial.” Even still, seventy-five percent of the former AUSAs felt that investigation and corroboration of cooperator’s information was sufficient to insure truthfulness. These blanket assertions were contradicted, however, when over half of the interviewees recounted instances where corroboration was insufficient to assure that convictions were based upon truthful information. Furthermore, over half of the former AUSAs expressed concern over what is considered “corroboration” in many cases. In other words, the cooperation game is by no means a science.

As the interviews continued, it became apparent that the cooperation system is inherently unreliable and that it is easy to be fooled by the average cooperator. This is particularly true in the white-collar context, several noted, where there are often facts that cannot be corroborated. For example, one interviewee explained that if a CFO agrees to testify that the CEO knew a certain fact on a certain date based on a conversation they had, how do you corroborate that? And when you ask an accountant who deals with volumes of information on a daily basis to recall something from three months ago, where is the assurance that they’ll get it right? Often times, they explained, this sort of corroboration requires a leap of faith: if you can confirm that A and B did in fact have a conversation on the date that A claims, this may be enough to corroborate what A claims was the substance of that conversation. These “leaps of faith” seem more common than they should be.

Outside of insufficient corroboration, the interviewees recalled several other instances where they held a false belief in the truthfulness of a cooperator and

89. Id. at 921.
90. Yaroshesfky, supra note 72, at 931.
91. Id.
92. Id. (quoting Interviewee number nine) [hereinafter I-1--I-25]. All interviews are on file with Professor Yaroshesfky.
93. Id.
94. Id. at 932
95. Yaroshesfky, supra note 72, at 936.
96. I-15, supra note 93.
97. Id.
98. Id.
their purported reason for that belief. Among these reasons was that AUSAs failed to investigate cooperators’ claims. In the most recurring example, several AUSAs cited multiple cases where they failed to investigate a cooperator’s contention that he or she had filed or correctly filed tax returns.99 Most learned their lessons the hard way, however, when on cross-examination, talented defense counsel exposed the cooperating witness’ tax fraud and were able to undermine their credibility, and sometimes the prosecutions case.100

Another reason the AUSAs reported for relying upon untruthful cooperators was that they trusted specific cooperators and believed they could accurately assess their truthfulness.101 But with the power of hindsight, one explained: “By definition cooperators are manipulative. You must create an arm’s length relationship . . . You want the information and he wants the benefit. It is easy to be manipulated.”102 The AUSAs admitted that they have foolishly believed that cooperators are “on their team” and forget that they are just eager to please.103 One interviewee recounted a middle aged lady who seemed “so prim and proper” and claimed this was the first time she had acted as a drug courier.104 Of course, defense counsel exposed that she had done so many times before, and the AUSA quickly learned that anyone who had done something once had done it before.105

In a particularly instructive portion of the interviews, many of the AUSAs and defense attorneys reported instances where the prosecution had a rigid theory of guilt that clouded their judgment. This occurs most frequently, the interviewees explained, when the prosecution believes they have the guilty guy and, accordingly, tend to believe anything that fits into that theory and ignore anything that is inconsistent with it.106 Thus, cunning defendants are able to sense what prosecutors want them to say and lie to give it to them.107

In one outrageous example of this rigidity, a cooperator testified that he had been present when the defendant at issue received a gun and shot the victim.108 Hospital records reflected, however, that the defendant had been hooked up to an IV during the evening in question and that he was checked on every hour. And although it seemed clear that the cooperator had lied, the prosecution took the impossible position that the defendant had snuck out of the hospital to commit the crime in that small timeframe.109 This was, the former AUSA recounted, a

99. See I-3, supra note 93; I-15, supra note 93; I-17, supra note 93; I-18, supra note 93; I-24, supra note 93.
100. Yaroshefsky, supra note 72, at 940 (quoting I-3, supra note 93; I-17, supra note 93).
101. Id. at 943.
102. I-8, supra note 93.
103. Yaroshefsky, supra note 72, at 940.
104. I-8, supra note 93.
105. Yaroshefsky, supra note 72, at 941.
106. Id. at 945.
107. I-16, supra note 93.
108. Yaroshefsky, supra note 72, at 946 (citing I-2, supra note 93).
109. Id.
classic example of a young prosecutor “buying his own bullshit.” 110 There was no shortage of these sorts of examples, as one defense attorney recalled an AUSA telling his client that if he simply dreamed being at the scene of a crime with the defendant, he would get his 5K1.1 letter. 111 These anecdotes also make it easy to see how an AUSA could abuse this power to bend a verdict in his favor.

Of the other reasons the interviewees gave for falling for a cooperator’s lies were cultural barriers, the attitudes of individual AUSAs, and lack of experience. On cultural differences, one AUSA described a money laundering case in which all of his cooperators were Chinese businessmen whose body language and tone of voice were impossible to read. 112 Regarding AUSA attitudes, several interviewees reported working with enforcement-minded AUSAs who identified with agents and seemed willing to push the margins to put bad guys away. 113 And with respect to lack of experience, many described young, albeit talented, AUSAs who lacked the street smarts or life experience to discern the mistake makers from the actual bad guys. 114

Looking at the results of the interviews, it is undeniable that cooperator deceit and prosecutorial naïveté are problem within the criminal justice system that warrants further study and, potentially, reform. 115 Perhaps USAOs would benefit by evaluating AUSA candidate not only by their ability to write a thirty-page brief, but also upon their deftness in human interactions and their internal “bs meter.” Professor Yaroshefsky’s findings are nonetheless insightful and instructive for current or future AUSAs. More pertinent to this article, the intangible skills they emphasize as important are certainly great talking points for someone, like myself, who hopes to apply to a USAO in the near future.

III. WHITE COLLAR DEFENDANTS AND ASSET FORFEITURE

Your client, Joe Doctor, owns and operates a pain relief clinic in Southwestern Ohio. Doctor manages the clinic and hires doctors as independent contractors to work under him and prescribe medication to patients on a need-only basis. Cognizant that pain relief clinics have recently come under fire in the news for allegedly operating as “pill mills” – facilities that operate under the guise of a providing legitimate pain treatment but that illegally prescribe opiate-based medications to nearly anyone who walks through the door – he makes sure that his doctors prescribe medication legally. Doctor maintains an open-door policy with local law enforcement because he feels he has nothing to hide. But

110. Id.
111. Id.
112. Yaroshefsky, supra note 72, at 946 (citing I-15, supra note 93).
113. Id. at 949.
114. Id. at 951 (citing I-20, supra note 93; I-15, supra note 93; I-21, supra note 93; Eugene M. Fodor & Terry Smith, The Power Motive as an Influence on Group Decision Making, 42 J. PERSONALITY & SOCIAL PSYCHOL. 178, 178-84 (1982)).
115. Id at 921.
after Doctor’s clinic brings in a healthy sum of money in one fiscal year, questions start getting asked.

Doctor learns he is being investigated by the Drug Enforcement Agency (“DEA”) and decides to be fully cooperative. He contacts you and, just in case the local USAO decides to bring charges against him, requests that you begin your own investigation and prepare to fight any charges. Given how much business Doctor’s clinic has done, this task is daunting and expensive. But you are aware of Owner’s net worth, so you accept and begin mounting a defense against any charges that may follow.

One year later, a grand jury indicts Joe Doctor on several counts, one of which is money laundering. The USAO takes the indictment to a district court judge and seeks ex parte forfeiture of any of Doctor’s assets that traceable to the underlying charges. The judge grants the forfeiture, and, suddenly, Doctor is unable to continue affording counsel – not to mention pay the hefty legal bill your racked up over the past year. The millions Doctor has made is gone. Almost all of his assets are gone. And up to this point, Doctor has not had an opportunity to be heard or challenge probable cause of any of the charges against him.

After the Sixth Circuit’s decision in United States v. Jamieson, this is an all-too-real predicament that criminal defendants (particularly white-collar) within the circuit face. Fortunately, the tides may be changing.

On the 50th anniversary of Gideon v. Wainwright – the landmark Supreme Court decision establishing indigent defendants’ right to counsel – the high court is addressing a federal circuit split on the seldom-referenced right to counsel of choice. The Sixth Amendment right to counsel of choice guarantees defendants the right to be represented by an attorney of their choice (i.e., one they can afford to hire). Unlike the right to counsel, which is typically invoked by those unable to afford an attorney, defendants (often white-collar) invoking their right to counsel of choice often enjoy significant financial means. That is, before the government seizes their assets in an ex-parte hearing, thereby effectively forcing upon them a court-appointed attorney.

Argued in October, the issue before the Supreme Court in Kaley v. United States is whether the Fifth and Sixth Amendments require a pre-trial hearing at which a defendant may challenge probable cause of the underlying charges against him and, thus, the validity of the asset seizure. Resolution of this question is especially critical to white-collar defendants’ ability to continue paying their attorney – an attorney with whom they have developed a relationship and knows their case.

A. The Circuit Split

The counsel-of-choice circuit split stems from the Supreme Court’s decision in United States v. Monsanto,\textsuperscript{120} which held that the government may restrain a defendant’s assets prior to trial only upon showing probable cause that the assets are subject to forfeiture. Although a laudable ruling, it left open the issue of “whether the Due Process Clause requires a hearing before a pretrial restraining order can be imposed.”

On that question, seven Circuits hold that due process requires an adversarial, pre-trial hearing to determine whether there exists probable cause that the defendant is guilty of the underlying charges and that the assets at issue are subject to forfeiture.\textsuperscript{121} The Sixth, Tenth, and Eleventh Circuits, on the other hand, are more government friendly and require only a “limited hearing” to determine whether the assets in question are “traceable” to the underlying charges.\textsuperscript{122}

B. Grand Jury Investigation

In early 2005, the petitioners, Kerri L. Kaley, a Johnson & Johnson, Inc. sales representative, and Brian Kaley, came under investigation for allegedly selling hospitals’ prescription medical devices (“PMDs”) on a gray market.\textsuperscript{123} The allegations suggested that the Kaleys had obtained and resold sutures, torcars, and other surgical devices that Johnson & Johnson had previously sold to several hospitals. Asserting that the PMDs were unwanted and given to them voluntarily, the Kaleys immediately retained counsel to represent them in what became a tedious two-investigation.

During the investigation, the Kaleys’ counsel undertook full examination and analysis of all relevant documents and circumstances, conferred with the prosecution, and began mounting a defense. The Kaleys quickly recognized an indictment was likely to follow and that the complex charges against them – further complicated by Johnson & Johnson’s burdensome return policies, which the Kaleys credit with creating the “gray market” at issue – would require significant time and money. Accordingly, they Kaleys applied for a credit line on their home and bought a $500,000 certificate of deposit (“CD”) to foot their legal bills through trial.

\textsuperscript{120} 491 U.S. 600 (1989).
\textsuperscript{121} Id.; United States v. Melrose E. Subdivision, 357 F.3d 493, 504-05 (5th Cir. 2004); United States v. Michelle’s Lounge, 39 F.3d 684 (7th Cir. 1994); United States v. Monsanto, 924 F.2d 1186 (2d Cir. 1991) (en banc); United States v. Roth, 912 F.2d 1131, 1134 (9th Cir. 1990); United States v. Lewis, 759 F.2d 1316, 1324 (8th Cir. 1985); United States v. Long, 654 F.2d 911, 915 (3d Cir. 1981).
\textsuperscript{122} Kaley II, 677 F.3d 1316 (11th Cir. 2012); United States v. Jamieson, 427 F.3d 394 (6th Cir. 2005); United States v. Farmer, 274 F.3d 800 (4th Cir. 2001) (applying the Mathews test, but limiting the hearing to traceability); United States v. Jones, 160 F.3d 641, 648 (10th Cir. 1998).
\textsuperscript{123} Petition for Writ of Certiorari, at 7; Kaley II, 677 F.3d at 1318.
C. Kaley I

In February 2007, a grand jury finally indicted the Kaleys for transporting “stolen” PMDs in interstate commerce, conspiring to transport “stolen” PMDs, and obstructing justice.124 Significantly, the indictment sought criminal forfeiture of all property traceable to the transporting charges. Two days later, a magistrate judge held an ex parte hearing – where only the prosecution was heard – and issued a restraining order to freeze a limited portion of the Kaleys assets. Unsatisfied with the limited restraint, the prosecution added a money-laundering charge to a superseding indictment in order to restrain any and all property that was “involved in” the charged crimes.125 With the added charge, the district court issued a restraining order on all $500,000 in the Kaleys’ CD. Again, the Kaleys had no opportunity to contest that there was probable cause for money laundering or any of the charges against them.

The Kaleys challenged the constitutionality of the restraint, arguing that they were entitled to a pretrial adversarial hearing where the government would have the burden of proving that it was likely to prevail at trial on the underlying charges. They argued that deprivation of the assets they needed to retain their counsel of choice without such a hearing was a violation of Due Process. The government opposed, arguing that under United States v. Bissell,126 the Kaleys could have, at most, a hearing to contest the tracing of the restrained assets to the crimes, but only if they proved that they could not retain counsel after liquidating all of their unrestrained assets over $500.

The district court agreed with the government, applying a four-factor test set forth in Barker v. Wingo,127 adopted in Bissell, to determine whether a pretrial, post-restraint hearing was required.128 The Barker factors asked the court to weigh: “(1) the length of the delay before the defendants received their post-restraint hearing; (2) the reason for the delay; (3) the defendants’ assertion of the right to such a hearing pretrial; and (4) the prejudice the defendants suffered due to the delay weighed against the strength of the United States’ interest in the subject property.”129 Emphasizing the government’s strong regulatory interest in preventing crime and challenges to indictments in advance of trial, the court held that the factors weighed against the Kaleys. Thus, the court held that there would not be an adversarial hearing of any sort. And because the Kaleys could no longer afford the counsel they had retained for over two years and throughout the

124. Kaley II, 677 F.3d at 1318.
125. Petition for Writ of Certiorari, supra note 124, at 7.
course of these proceedings, they took an interlocutory appeal to challenge this denial in the Eleventh Circuit. 130

On appeal to the Eleventh Circuit, the Kaleys contended that the district court misapplied the Barker factors and that, in either case, it should have applied the factors set forth in Mathews v. Eldridge, 131 not Barker. The Mathews test asks the court to weigh the (1) private interest affected by the restraint, (2) risk of erroneous deprivation through the procedures used and the probable value of additional procedural safeguards, and (3) the prejudice to the government. 132

Looking at Barkers and Mathews, the Eleventh Circuit explained that “[i]f we were writing on a blank slate today we would be inclined . . . to apply the test announced by the Supreme Court in Mathews.” 133 And although it felt bound by Bissell’s adoption of the Barker test, the court still reversed the district court, noting that it had misapplied the Barker factors and needed to “re-weigh” them. Judge Tjoflat concurred, however, finding that, under the Mathews test, the Kaley’s interests were significant. 134 Notably, he determined that the denial of an adversarial hearing would “eviscerate [the Kaleys] right to counsel of choice” and that neither a grand jury’s ex parte finding of probable cause nor an ex parte affidavit by the government were likely to protect defendants “against an erroneous deprivation.”

D. Kaley II

On remand, the district court applied the Barker factors and held that the Kaleys were entitled to a limited evidentiary hearing to determine whether the assets in question were traceable to the alleged crimes – identical in scope to the limited hearings allowed by the Sixth Circuit. 135 And because the Kaleys did not contest the traceability of its house and CD, the hearing was largely a formality. Consequently, they took a second interlocutory appeal.

The Eleventh Circuit answered this appeal by clarifying that at a “pretrial, post-restraint hearing required under the Bissell test, the petitioner may not challenge the evidentiary support for the underlying charges.” 136 It explained that, even where a defendant prevails under the Barker test, it may only challenge traceability. Yet, Judge Edmondson concurred “with deep doubts,” explaining

130. In their petition for writ of certiorari and briefs before the Supreme Court, the Kaleys repeatedly point to the acquittal of their co-defendant, Jennifer Gruenstra, to show that no probable cause could justify the government’s restraining order. See, e.g., Brief for Petitioners at 32, Kaley, 133 S. Ct. 1580 (No. 12-464).
133. Kaley I, 579 F.3d at 1259 (11th Cir. 2009).
134. Kaley I, 579 F.3d at 1262-65 (Tjoflat, J., concurring).
that, if he “were deciding the case alone,” that he would reach a different result and write something largely in line with Second and D.C. Circuit positions. As such, he opined that Due Process required an evidentiary hearing “about probable cause on . . . the predicate criminal offense” for such an asset restraint. Ending his opinion, he warned:

For the Federal Executive, in effect, to seize a citizen's property; to deprive him thereby of the best means to defend himself in a criminal case; and then, by means of the criminal case, to take his liberty strikes me as a set of circumstances about which our nation's history and its Constitution demands that the process at each step be fully fair. The potential for the dominating power of the Executive Branch to be misused by the arbitrary acts of prosecutors is real. The courts must be alert. To hear from the other side at a time when it matters (in this instance, before the criminal trial: a trial without counsel of the defendant’s choice) is the basic and traditional way that American judges assure things are fair.

And although the Kaleys’ petition for rehearing en banc failed, Judge Edmonson’s sharp words may have caught the attention of at least one court: the Supreme Court of the United States.

E. Supreme Court Proceedings

Taking occasion to address the “firmly entrenched split among the eleven circuits,” the Supreme Court granted the Kaleys’ petition for writ of certiorari to address their right Fifth and Sixth Amendment right to a pretrial, adversarial hearing to challenge the restraining order, entered ex parte, that froze the assets they needed to retain counsel. Having appeared before the Court in October, the Kaleys’ and the United States’ briefs on the merits reflect the parties principal arguments. Both parties have requested review.

The Kaleys have aligned their primary arguments with those accepted by the seven-circuit majority, arguing that Due Process mandates a pre-trial, adversarial hearing to establish probable cause of the underlying charges. The government asserts, in line with the minority, that, even if the Kaleys are entitled to a pretrial, adversarial hearing, the Eleventh Circuit correctly limited the scope of that hearing to traceability.

137. Kaley II, 677 F.3d at 1330 (Edmonson, J., concurring).
138. Id. at 1332.
139. Petition for Writ of Certiorari, supra note 124, at i.
141. Brief for Petitioners at 32, Kaley, 133 S. Ct. 1580 (No. 12-464).
1. Petitioners’ Arguments

The Kaleys assert that the Eleventh Circuit should have applied Mathews to determine whether they were entitled to an adversarial, pre-restraint hearing, and that as applied, they were. They explain that Barker only applies when a defendant seeks dismissal of the government’s case based on undue delay between restraint and trial, a delay inapplicable to the Kaleys. In support of their argument that Mathews requires an adversarial hearing on probable cause before a pre-trial restraint of assets, the Kaleys cite Connecticut v. Doehr and United States v. James Daniel Good Real Property.

The Doehr Court noted that no judge can adequately evaluate probable cause based on “one-sided, self-serving, and conclusory submissions.” Similarly, in James Daniel, the Supreme Court prevented the government from seizing a convicted criminal defendant’s home in anticipation of forfeiture proceedings until it established probable cause that the home was used to facilitate underlying crimes in an adversarial, pre-seizure hearing. The Supreme Court unabashedly cautioned that because forfeitures are a critical component of the government’s annual budget, they present a serious potential for abuse in need of safeguarding.

Drawing on the principles elicited in Doehr and James Daniels, the Kaleys present compelling arguments. First, they argue that their interest in preventing restraint is significant because such restraint deprives them of their property, thereby eviscerating their right to counsel of choice. Second, they claim that their assets, especially the $500,000 CD, face substantial risk of erroneous deprivation because the government has “direct pecuniary interest” in obtaining them. Further, unlike the defendant in Doehr, the Kaleys have not been convicted and maintain their innocence as to the underlying charges. Lastly, they contend that the government’s interest in avoiding an adversarial hearing is either negated by its post-hearing substantial discovery obligations, or protected by its ability to exercise prosecutorial discretion and forego interim asset restraint.

2. The United States Arguments

In its brief on the merits, the United States arguments are guided by two themes: (1) a grand jury’s finding of probable cause is, and has always been, 143. Brief for Petitioners, supra note 142, at 46 (citing Barker, 407 U.S. at 530 (1972) (asking courts to consider: length of delay, the reason for the delay, the defendant's assertion of his right, and prejudice to the defendant)).
144. Id. at 51-52, 64.
146. Id.
147. Brief for Petitioners, supra note 142, at 51-63.
immune from the proposed inquiry, and; (2) the Kaley’s interest in retaining their
counsel of choice pales in comparison to the government and public’s interest in
preserving forfeitable assets.149

With regards to the former, the government maintains that a rule of criminal
procedure – like a defendant’s inability to contest an indictment – does not
violate due process unless it offends a fundamental principle of justice.150 And
where grand-jury determinations are sacrosanct in our system of justice, it
argues, the Sixth Amendment right to counsel of choice does not
Finally, it
contended that adversarial, probable-cause hearings present prosecutors with a
catch-22: prematurely disclose the government’s case and trial strategy, thus
jeopardizing the safety of witnesses; or forego restraint, leaving the government
no means to prevent the depletion of contested assets.151

F. Awaiting an Answer

Twenty-four years after it decided that the government may not restrain
criminal defendant’s assets without probable cause, the Supreme Court will
finally address the question it left open in Monsanto: does due process require an
adversarial hearing before such restraint can be imposed? A “yes” will ensure
that criminal defendants have an opportunity to contest the restraint against them
in a meaningful manner. More importantly, it will secure their right to choose
their counsel and preserve the adversariness that is fundamental to our system of
justice. As one of the circuits in the minority, this decision is critical to the Sixth
Circuit and its white-collar defendants.

IV. CONCLUSION

In my short, short legal career, I have had the privilege of a top-notch
education and meaningful experiences that few law students will share. So
accepting my litigation-minded nature, it is only appropriate do whatever I can to
put my past two-and-a-half years to use in a manner that seems most appropriate:
litigating. With an eye towards my ultimate goal of doing just that in federal
court, I drafted this paper to verse myself in recent changes in white-collar
criminal law – changes that I, guided by my legal education and relevant
experience, deemed most relevant to the actual practice of white-collar crime.
Had I not been a party to such valuable experiences, I would not have realized
what issues are important in this field; had I not been a full-time student of the
law, I may not have discovered that these issues are currently undergoing
changes and been able to thoroughly research these changes.

Having witnessed a pre-arrest interview about a client suspected of white-
collar crimes, I recognized the importance of behavior in interviews. An

149. See generally Brief for the United States, supra note 149.
150. Id. at 22.
adequately prepared client can silence governmental concerns and, literally, “clear his name”; but by the same token, an unprepared or misinformed client can quickly turn himself from a potential witness into a suspect. The Supreme Court’s recent decision *Salinas v. Texas* further complicates pre-arrest interviews by clarifying that the well known “right to remain silent” is not as absolute as it sounds. By allowing prosecutor’s to use a suspect’s pre-arrest silence against him at trial, *Salinas* gives the government another tool to use to convict criminals and gives defendants another reason not to cooperate with police. Criminal litigators need to understand this.

Moreover, by watching talented AUSAs and defense attorneys eagerly cooperate with one another, I realized that substantial assistance letters are a dynamic tool for both sides of the law. Substantial assistance recommendations not only allow the government to gather information in cases that would otherwise be impossible to prosecute, but they allow defense attorneys to drastically reduce their client sentences. So by acquainting myself with the manner by which these letters are given and, through Professor Sharotefsky’s groundbreaking research, the psychology of the AUSAs writing them, I am prepared to partake in the cooperation process and avoid the mistakes of AUSAs before me.

Lastly, seeing that a client’s defense could crumble in light of a momentous asset-forfeiture, I can appreciate and anticipate the power of money laundering charges. But as an aspiring attorney who will practice within the Sixth Circuit, I eagerly await the Supreme Court’s decision in *Kaley v. United States*. If the *Kaley* court overturns the view held by the Sixth Circuit, I will understand that AUSAs must be prepared to defend the probable cause for any asset forfeitures they seek, even if that means “showing their cards” before trial. On the other side, overturning the Sixth Circuit would present defense attorneys with a new opportunity to meaningfully challenge asset forfeiture. Either outcome is something that all white-collar crime attorneys should aware of.

However, there is no certainty as to where I end up in my legal career. Plans do change, and perhaps I may be destined for a career in divorce law. But in either case, I now have valuable knowledge that can help me in my career. And now matter where I end up, hopefully one white-collar client walks through my door and asks for advice.
THE CLOUD OF WAR: SECURING THE OPERATIONAL DOMAIN OF CYBERSPACE WITH A ROBUST MILITARY COMMAND

Erica Hauck

The traditional military command structure has evolved over time to adapt to the international community’s war-fighting domains. Recently, the United States government recognized cyberspace as an operational domain where war can be waged. Cyberspace is unlike any of the traditional domains for which military commands have adapted. As a result, customary international law is inadequate to govern cyberspace and cyber warfare. Yet, because the presidential administration recognizes cyberspace as a war-fighting domain, the Department of Defense must be responsible for leading the efforts to secure U.S. cyberspace. In order to effectively operate in this relatively new domain, the U.S. military’s combatant command structure for cyberspace must employ both domestic intelligence and private sector resources. Although Congress and the American people are concerned that additional governmental operations in cyberspace will encroach upon Americans’ privacy rights and civil liberties, securing cyberspace requires a robust collaboration between the Department of Defense, the Department of Homeland Security, and the private sector.

I. INTRODUCTION

Because cyberspace is unlike any of the existing domains where the U.S. wages war and defends the nation, it requires an innovative command structure unlike a traditional military combatant command. To accomplish this, the military combatant command responsible for defending cyberspace must exercise more control over U.S. intelligence-gathering agencies and the private sector. The threat of cyber war has catapulted to national prominence during the current presidential administration.¹ For example, current Secretary of Defense Chuck Hagel revealed that the U.S. “is dangerously exposed to cyberspace attacks.”² Because cyberspace is such a new and complex domain, it is difficult to categorize modern cyber threats. The current presidential administration recently defined cyberspace as “[t]he interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computers, information or communications systems, networks, and embedded infrastructures.”

¹. See DEP’T OF DEF. STRATEGY FOR OPERATING IN CYBERSPACE 1 (July 2011), available at http://www.defense.gov/news/d20110714cyber.pdf (“From 2000 to 2010, global Internet usage increased from 360 million to over 2 billion people.”).
processors and controllers.”

Ironically, this definition was not meant for dissemination; instead, staff writers at a United Kingdom-based media outlet leaked a Top-Secret Presidential Memorandum on June 7, 2013. Nonetheless, this leaked Presidential Policy Directive confirmed that the President aims to strengthen U.S. offensive cyber war capabilities. Unlike more discernible threats to U.S. National Security, cyberspace “disrupts the traditional threat taxonomy” and makes systems designed to protect against traditional threats less effective. Hence, the complex nature of cyberspace and its differences from traditional operational domains will require the U.S. Department of Defense (DoD), and specifically U.S. Cyber Command (USCYBERCOM), to lead the nation’s cyber capabilities and share information with national intelligence agencies and the private sector.

Part II of this Note provides background into the traditional military combatant commands, as well as USCYBERCOM as an emerging combatant command. Part III points out that USCYBERCOM is not currently equipped to effectively operate in cyberspace. Part IV proposes changes to make USCYBERCOM a more effective combatant command. Finally, Part V provides concluding remarks.

II. BACKGROUND

The U.S. Constitution grants power to both the President and Congress to defend the nation. The President can delegate his constitutional executive and commander-in-chief powers “through the Secretary of Defense down to

---


4. See Obama Tells Intelligence Chiefs, supra note 3.


6. See Susan W. Brenner, Cyber-Threats and the Limits of Bureaucratic Control, 14 MINN. J.L. SCI. & TECH. 137, 144 (2013) (describing traditional threat categories as crime, terrorism, and warfare). “Cyberspace erodes those distinctions” between crime, terrorism, and warfare, which are otherwise “reasonably well defined and reasonably stable in the physical world.” Id.


8. U.S. CONST. art. I, § 8 (granting Congress the power to “declare war,” “raise and support Armies,” “provide and maintain a Navy”); U.S. CONST. art. II, § 2, cl. 1 (mandating the “President shall be Commander in Chief of the Army and Navy of the United States”).
subordinate commanders.” Accordingly, DoD provides military forces to deter war and protect U.S. security. In order to effectively provide these military forces, DoD has divided its military forces into nine unified combatant commands. By dividing responsibility into commands, DoD “support[s] U.S. defense security commitments around the world while improving military responsiveness to emerging crises.” Of the nine U.S. military combatant commands, six are regional and divided according to “geographic areas of responsibility.” Each of these six regional combatant commands has an area of responsibility (AOR). The remaining three commands are assigned functional responsibilities.

A. Traditional Combatant Commands

1. Areas of Responsibility

Six of DoD’s nine unified combatant commands are divided according to “geographic areas of responsibility.” Each regional combatant command is

---


11. See 10 U.S.C. § 161 (2006) (defining “unified combatant command” as “a military command which has broad, continuing missions and which is composed of forces from two or more military departments.”). By law, the President has the authority to establish a unified combatant command, and there is no limitation on the number of commands that he can establish. Id. Except during time of hostilities or imminent threat of hostilities, however, the President must notify Congress within 60 days of establishing a new combatant command. Id. (b)(2).


13. See Unified Command Plan , supra note 12 (“The Unified Command Plan establishes the missions and geographic responsibilities among the combatant commanders.”). The Unified Command Plan is a top-secret document that “establishes the missions and geographic responsibilities among the combatant commanders.” Unified Command Plan , supra note 12.

14. Unified Command Plan, supra note 12. The six regional areas are: North America (USNORTHCOM), South America (USOUTHCOM), Europe (USEUCOM), Africa (USAFRICOM), the central area of the globe (USCENTCOM), the Pacific (USPACOM), and space operations (USSTRATCOM). Unified Command Plan, supra note 12.


16. See Unified Command Plan, supra note 12. (noting that the functional commands include USTRANSCOM (Transportation) and USSOCOM (Special Operations)). Although USSTRATCOM is considered a regional combatant command because its area of responsibility includes outer space, it also possesses many functional capabilities, such as “combating weapons of mass destruction” and “computer network operations.” U.S. TRANS. COMMAND, Public Combatant Commands, http://www.transcom.mil/about/combatant.cfm (last visited Apr. 5, 2014).

17. Uniform Command Plan, supra note 12 (noting that the Chairman of the Joint Chiefs of Staff reviews the geographical boundaries of each combatant command every two years and
responsible for “maintaining superiority across the range of military operations in all domains” within its AOR.\textsuperscript{18} To illustrate, U.S. Pacific Command’s (USPACOM) AOR “encompasses approximately half the earth’s surface and more than half its population,” including the thirty-six nations that comprise the Asia-Pacific.\textsuperscript{19} Like the other military combatant commands, USPACOM’s priority is maintaining its superiority as a war-fighting command; thus, it must exercise control “across the range of military operations in all domains,” which are made up of sea, air, space, and cyberspace.\textsuperscript{20} To accomplish this, USPACOM’s missions seek to maintain “interoperable military capabilities in the region.”\textsuperscript{21}

In addition to the six regional combatant commands, DoD has three additional combatant commands with functional capabilities.\textsuperscript{22} While these commands do not have defined geographical AORs, they provide support to the “other U.S. combatant commands, the military services, defense agencies, and other government organizations.”\textsuperscript{23} For example, U.S. Transportation Command (USTRANSCOM) is responsible for, among other duties, providing “transportation, sustainment and distribution” to DoD to support both peace and wartime duties.\textsuperscript{24}

2. Lines of Operation

Within a combatant military command, a military force is “designed using lines of operation.”\textsuperscript{25} Forming the basis for major combat operations, lines of operation tie together tasks and actions into a sequence to achieve the mission.\textsuperscript{26} Typically, military combatant commanders “synchronize activities along multiple

\begin{footnotesize}
\begin{enumerate}
\item U.S. PAC. COMMAND, Strategy, supra note 18. Similarly, U.S. Central Command’s (USCENTCOM) AOR covers the “central” area of the globe and consists of twenty countries. U.S. CENT. COMMAND, supra note 15.
\item See U.S. PAC. COMMAND, Strategy, supra note 18.
\item U.S. PAC. COMMAND, Strategy, supra note 18.
\item See U.S. TRANSP. COMMAND, Public Combatant Commands, http://www.transcom.mil/about/combatant.cfm (last visited Apr. 5, 2014) (including in the listing of commands the functional combatant commands U.S. Transportation Command (USTRANSCOM) and U.S. Special Operations Command (USSOCOM)).
\item What is USTRANSCOM?, supra note 23.
\item Pellerin, supra note 3; See also Center for Army Lessons Learned - Thesaurus, http://usacac.army.mil/cae2/call/thesaurus/toc.asp?id=34073 (last visited Aug. 9, 2013) (defining a line of operation as “the directional orientation of a force in time and space in relation to the enemy and links the force with its base of operations and objectives”).
\item See Center for Army Lessons Learned - Thesaurus, supra note 25.
\end{enumerate}
\end{footnotesize}
and complementary” lines of operation “through a series of military strategic and operational objectives to attain the military end state.” 27 A line of operation distinctly consists of a “series of actions executed according to a well-defined sequence.” 28 When designing a major combat operation, commanders have numerous tools upon which to rely, including two types of lines of operation. 29 First, a physical line of operation “defines the interior or exterior orientation of the force in relation to the enemy or connects actions on nodes and/or decisive points related in time and space to an objective(s).” 30 Second, a logical line of operation “connects actions on nodes and/or decisive points related in time and purpose with an objective(s).” 31

In practice, a regional combatant commander focuses on specific objectives from which to design the lines of operation. Illustratively, U.S. Marine Corps General James N. Mattis, Commander of USCENTCOM, focused on “four main drivers of U.S. foreign policy” when designing his approach to USCENTCOM’s military activities within its AOR. 32 It is reasonable to assume that, from those four drivers, the commander will utilize both physical lines of operation and logical lines of operation to construct his military force. 33 Over time, the various sequences of lines of operation have adapted to execute missions in both war and peacekeeping missions throughout traditional operational domains. 34

3. Waging War with a Traditional Combatant Command

The military combatant commands have designed and executed their missions pursuant to existing international laws of war. The United Nations

27. Center for Army Lessons Learned - Thesaurus, supra note 25.
28. Center for Army Lessons Learned - Thesaurus, supra note 25.
29. See Center for Army Lessons Learned - Thesaurus, supra note 25 (“Normally, joint operations require commanders to synchronize activities along multiple and complementary physical and logical [lines of operation] working through a series of military strategic and operational objectives to attain the military end state.”).
30. Center for Army Lessons Learned - Thesaurus, supra note 25.
31. Center for Army Lessons Learned - Thesaurus, supra note 25.
33. See Wall, supra note 9, at 91 (“Most details of how [unconventional and cyber warfare] operations are conducted are not publicly available.”); see also John Arquilla, Cyberwar is Already Upon Us, FOREIGN POLICY (March/April 2012), http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us (“Most information on cyberwar’s repercussions . . . remains classified.”). An assumption is necessary here because, while lines of operation are doubtlessly being employed, the details of those operations are classified. See id. However, both physical and logical lines of operation in similar operations parallel modern circumstances faced by the regional combatant commands. Id.
(U.N.) Charter generally outlawed war and the use of force in Article 2(4). Over time, the U.N. Charter has raised questions of interpretation; notably, what constitutes a “use of force”? For example, the International Court of Justice (ICJ) has contemplated the threshold an armed attack must meet to trigger a nation’s right to self-defense. The ICJ determined that Iranian missiles and mining activities did not constitute an armed attack on the U.S. when they damaged U.S. ships because that damage did not meet the court’s requirement of a “most grave” form of the use of force. Thus, the ICJ determined that Iranian activity did not rise to the level of an armed attack.

The drafters of the U.N. Charter included two exceptions to the prohibition against the use of force or threat of use of force. One exception is a nation’s right to self-defense. Under Article 51 of the U.N. Charter, self-defense is appropriate if an armed attack has already occurred against a U.N. member. The traditional view is that Article 51 complements Article 2(4), creating an exception to the general prohibition of force. Moreover, because attacks by military forces are generally illegal, “armed self-defense is permissible only if alternative measures are insufficient to defend a threatened sovereign right.”

---

35. U.N. Charter art. 2, para. 4. Article 2(4) of the U.N. Charter mandates that all U.N. members “shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.” Id.


37. Sheng Li, supra note 36, at 185 (citing Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 35 (June 27) (“Only acts of aggression of sufficient ‘scale and effects’ constituted armed attacks.”)).

38. Sheng Li, supra note 36, at 185 (quoting Oil Platforms (Iran v. U.S.), 2003 I.C.J. 90, ¶ 51 (Nov. 6)).

39. Sheng Li, supra note 36, at 185 (citing Oil Platforms (Iran v. U.S.), 2003 I.C.J. 90, ¶ 51, 64 (Nov. 6)).

40. See Schachter, supra note 36, at 1620 (noting that the U.N. provides exceptions for “force used in self-defense when an armed attack occurs, and armed action authorized by the U.N. Security Council as an enforcement measure”).

41. See Sheng Li, supra note 36, at 183 (“Articles 2(4) and 51 of the U.N. Charter govern the modern law of self-defense.”).

42. U.N. Charter art. 51; see also Sheng Li, supra note 36, at 184 (citing Yoram Dinstein, WAR, AGGRESSION AND SELF-DEFENSE 85–86 (2011)).

43. Waxman, supra note 36, at 427. Specifically, “Article 51 carves out the exception to Article 2(4)’s otherwise strict prohibition of force.” Id. (citing Thomas M. Franck, RECURS TO FORCE: STATE ACTION AGAINST THREATS AND ARMED ATTACKS 45-52 (2002)).

44. Waxman, supra note 36, at 422.

Thus, the law limits self-defense to that force which is necessary for defeating the threat. Additionally, the existing international law principle of *jus ad bellum* requires force used in self-defense to be proportional to the initial attack. Hence, in uses of force in self-defense, a lawful response must meet the requirements of necessity and proportionality.

**B. U.S. Cyber Command: A Non-traditional Combatant Command**

The U.S. Secretary of Defense ordered the establishment of USCYBERCOM on June 23, 2009, as a sub-unified command subordinate to U.S. Strategic Command (USSTRATCOM). USSTRATCOM is one of DoD’s nine unified combatant commands. In terms of its war-fighting domain, USSTRATCOM commands space operations. Importantly, USCYBERCOM is co-located with the U.S. National Security Agency (NSA), and the Director of the NSA also serves as the Commander of USCYBERCOM. USCYBERCOM is charged with “planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the DoD information networks.” Additionally, USCYBERCOM can “conduct[] full-spectrum military cyberspace operations . . . in order to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries.” By establishing USCYBERCOM, DoD sought to create relationships with other agencies to improve responses to attacks in cyberspace.

---

46. See Sheng Li supra note 36, at 183.
50. See U.S. STRATEGIC COMMAND, supra note 49 (“USSTRATCOM combines the synergy of the U.S. legacy nuclear command and control mission with responsibility for space operations.”).
51. DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE, supra note 1, at 5. USCYBERCOM was intentionally structured to “allow DoD, and the U.S. government, to maximize talent and capabilities, leverage respective authorities, and operate more effectively to achieve DoD’s mission.” Id. at 6.
52. U.S. Cyber Command Fact Sheet, supra note 48.
54. DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE, supra note 1, at 5. Specifically, USCYBERCOM will “ensure the development of integrated capabilities by working closely with Combatant Commands, Services, Agencies, and the acquisition community to rapidly deliver and
Currently, USCYBERCOM is tasked with coordinating each military branch’s cyber component. Moreover, one of USCYBERCOM’s strategic initiatives provides that “DoD will partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy.” One important step toward interagency collaboration was the “2010 memorandum of agreement signed by the Secretary of Defense and Secretary of Homeland Security to align and enhance cybersecurity collaboration.”

1. Area of Responsibility

Cyberspace has officially been recognized as a U.S. military operational domain. By categorizing cyberspace as an operational domain, DoD can establish an organizational foundation and prepare the appropriate forces. Cyberspace is revolutionary because it is the first instance where a non-physical space has been considered a war-fighting domain. Accordingly, cyberspace must be treated as its own operational domain because it differs so greatly from the traditional war-fighting domains. Even though cyberspace has been considered a war-fighting domain, there is no official definition of “cyber
warfare."\footnote[62]{See Bradley Raboin, \textit{Corresponding Evolution: International Law and the Emergence of Cyber Warfare}, 31 J. NAT’L ASS’N ADMIN. L. JUDICIARY 602, 603 (2011).} To date, the U.S. has not categorized any attack as cyber warfare, even though there have been acts that have threatened U.S. national security.\footnote[63]{See Wall, supra note 9, at 122 (citing James Andrew Lewis, \textit{Cyber Events Since 2006}, CSIS (Jan. 25, 2011), available at http://dev.csis.org/publication/cyber-events-2006) (noting that there have been "minor skirmishes, a silent cyber arms race, and major intelligence gathering").} Without a doubt, the Presidential administration is anticipating the onslaught of cyber warfare.\footnote[64]{See Obama Tells Intelligence Chiefs, supra note 3.}

2. Lines of Operation


3. Waging War with USCYBERCOM

Just as it is difficult to categorize the different types of cyber threats, it is unclear what type of attack will constitute an act of war in cyberspace. Adding to the complexity, there is no official definition of “cyber warfare,”\footnote[71]{See Raboin, supra note 62, at 603 (“The lack of workable, universally accepted definitions of cyberspace and cyber warfare only further exacerbates any attempt to analyze international regulation of activities, such as cyber warfare, occurring within the cyberspace domain.”).} and the definitions among U.S. governmental departments vary. On the one hand, DoD
has defined “cyber operations” as “the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace.” The Congressional Research Service, however, gave a more generalized definition of cyber warfare that focused on any “defending and attacking information and computer networks in cyberspace,” including the ability to deny an adversary to perform the same function. Although the proportionality requirement of *jus ad bellum* under customary international law applies to cyberspace, it is generally accepted that “[t]here is no legal requirement that the response to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality.”

Cyber attacks can be divided into multiple categories, such as malware, denial-of-service (DOS) attacks, and unauthorized intrusion. For example, a DOS attack can shut down a website by “overwhelm[ing] it with information until it seizes and can no longer function.” Cyber attacks can also illegally extract classified data to steal an individual’s identity. Intricately, much of the cyber technology now thought to be capable of cyber warfare has traditionally been espoused as espionage activity. Overall, the myriad of cyber threats the U.S. faces can not only be categorized as cyber warfare, by also as many other illegal international practices.

---


73. Raboin, supra note 62, at 609 (citing Steven A. Hildreth, Cong. Research Serv., RL30735, *Cyberwarfare* (2001)).


III. A TRADITIONAL COMBATANT COMMAND IS NOT EQUIPPED TO EFFECTIVELY SECURE CYBERSPACE

A. The Challenging Domain of Cyberspace

Most of cyberspace’s challenges stem directly from the domain of cyberspace itself. Currently, the Internet allows for many types of malicious activities that, despite constituting discernible threats to U.S. national security, do not constitute acts of war. On one end of the spectrum lie the individuals or small groups of cyber actors who, using widely available hacking tools, can “potentially cause significant damage to both DoD and U.S. national and economic security.” In contrast, a threat or use of force against another state is considered an act of war, allowing the victim-state to counter-attack. Intricately, because only states enjoy the right to self-defense, private sector firms who are victims of a cyber attack cannot “respond” to a cyber attack under international law, regardless of severity.

Even though cyberspace is unlike any of the existing war-fighting domains, international law applies to cyberspace. In some instances, it is clear when an act in cyberspace constitutes a use of force under Article 2(4) of the U.N. Charter and existing international law. If a cyber attack causes physical destruction, much like a bomb, it fits within the parameters “as a traditional kinetic attack.” In that sense, a cyber attack could easily be considered a “new weapon, means, or method of warfare” that is prohibited under Article 36, Additional Protocol I, of the Geneva Convention, because the result is the same as an existing method of warfare.

---

79. See Parrish, supra note 2 (“[Cyberspace] is a fundamentally different, more insidious kind of threat than we’ve ever seen – one that carries with it a great risk of miscalculation and mistake.”).
80. See Waxman, supra note 36, at 422 (“Definitions of cyber-attacks vary, and the range of hostile activities that can be carried out over information networks is immense, ranging from malicious hacking and defacement of websites to large-scale destruction of the military or civilian infrastructures that rely on those networks.”).
81. See DEP’T OF DEF. STRATEGY FOR OPERATING IN CYBERSPACE, supra note 1, at 3.
82. See U.N. Charter art. 2, para. 4.
84. Koh, supra note 74.
85. See Koh, supra note 74. One example that is commonly cited as a “use of force” under international law is a cyber attack that caused the same physical damage as a dropped bomb or fired missile. Id.
Conversely, other cyber attacks do not clearly fit within the international laws of war, and legal advisors have debated what type of attack constitutes a “use of force” under the U.N. Charter. One view is that an attack without physical consequences can never constitute a “use of force” under international law. However, DoD has affirmed that it will treat cyber attacks as uses of force and retaliate with a conventional military response. It seems clear that cyber attacks can “elevate to the matter of national security,” even without physical destruction. For example, the impact of a cyber assault on Estonia in 2007 amounted to “the provision of state benefits and the collection of taxes [were brought] to a halt, private and public communications were disrupted, and confidence in the economy plummeted.”

Some of the known challenges to cyberspace include the fact that “attacks are invisible, hard to track to their source, and potentially can be classified as either criminal activity or acts of war.” The U.N. Charter’s prohibition against the use of force applies when a threat is communicated, either explicitly or implicitly. Additionally, a counterattack against an unlawful use of force must be directed at a state actor. Yet in cyberspace, both state and non-state actors can act anonymously to launch an attack. Thus, the difficulty in attributing a

88. For example, “[c]yber espionage aims to obtain confidential information over the Internet,” and does not clearly fit the definition of “force” under the U.N. Charter. McGavran, supra note 86, at 262. “Currently, the law of war applies to cyber attacks by analogy only.” Id. at 269; Gabriel K. Park, supra note 75, at 800 (“It is unclear whether the current international legal regime can govern cyberattacks.”).

89. As the Commander of USCYBERCOM discussed during his Senate confirmation hearings, “[t]here is no international consensus on a precise definition of a use of force, in or out of cyberspace. Consequently, individual nations may assert different definitions, and may apply different thresholds for what constitutes a use of force.” Schmitt, supra note 83, at 573 (citing Staff of S. Comm. on Armed Services, Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command from the United States’ Armed Services Committee (Apr. 15, 2010), available at www.senate.gov/~armed_services/statemnt/2010/04%20April/Alexander%2004-15-10.pdf [hereinafter Advance Questions]).


91. Li, supra note 36, at 181 (“The prevailing consensus among scholars and policymakers holds that, because [distributed DOS] attacks cause neither physical nor destruction, they can never constitute armed attacks that trigger self-defense rights.”).

92. See Mazzetti, supra note 90 (discussing USCYBERCOM’s role in defending the nation if it is attacked in cyberspace).

93. Park, supra note 75, at 803.
94. Schmitt, supra note 83, at 570.
95. Parrish, supra note 2.
96. Schmitt, supra note 83, at 572.
97. See Li, supra note 36, at 202; see also Schmitt, supra note 83, at 575.
98. Park, supra note 75, at 797.
cyber attack to its origin makes it difficult to determine whether a cyber attack constitutes a use of force. For example, when Estonia suffered from a series of distributed DOS attacks in 2007, it initially traced the attacks to Internet Protocol (I.P.) addresses linked to Russian nationalist groups, but also linked the attacks “at least 177 other countries.” Estonia later attributed the attacks to the Kremlin; however, “there is no firm evidence that the Russian government either conducted or orchestrated” the attacks.

B. The Challenging Command of USCYBERCOM

Currently, USCYBERCOM is tasked with “defend[ing] military information networks against cyber attacks.” Moreover, because USCYBERCOM is part of DoD, it must also defend the homeland. Thus, when establishing the command, Secretary of Defense Robert Gates left room for vast expansion within USCYBERCOM. In addition to its function as an operational combatant military command, USCYBERCOM has the responsibility to “function as a supporting command to the national command authority at the Department of Homeland Security (DHS),” a role that is distinct from other traditional military commands. This creates a problem because “DoD has no authority to enforce military doctrines outside of the Department.” Clearly, this raises issues that are not often explored within a traditional combatant command. For

99. Li, supra note 36, at 202 (citing David Wheeler & Gregory Larsen, Techniques for Cyber Attack Attribution (2003)).
100. See Schmitt, supra note 83, at 575 (“[V]ery few states have definitively been identified as the initiator of a cyber operation that might amount to a use of force.”).
101. See Schmitt, supra note 83, at 569-70 (The massive computer network attacks compromised “information systems for everything from banking and filing tax returns to paying for parking and public transportation.”).
103. Schmitt, supra note 83, at 570.
104. Li, supra note 36, at 180 (citing Charles Clover, Kremlin-Backed Group Behind Estonia Cyber Blitz, FIN. TIMES (Mar.11, 2009), http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html).
105. Schmitt, supra note 83, at 570.
107. Pellerin, supra note 3 (“As part of DOD, . . . part of Cybercom’s mission is to help in defending the homeland, especially against cyberattacks and other activities in cyberspace that could affect national security.”).
108. See Young, supra note 106, at 174 (“Although the Cyber Command is not currently defending the civilian or commercial networks, this option may soon be considered necessary.”).
110. More commonly, the combatant military commands work closely with the foreign U.S. intelligence community, which does not have domestic jurisdiction. See ABOUT CIA, https://www.cia.gov/about-cia/faqs (last visited Aug. 9, 2013).
111. Young, supra note 106, at 175.
example, within a regional combatant command, all domains in the command’s specific area of operation (AOR) fall within the responsibility of that command. Yet, each combatant command works with other military branches and the intelligence community to effectuate operations across all domains. Unlike the regional combatant commands, USCYBERCOM focuses on one domain with a boundless AOR. Consequently, USCYBERCOM’s role as a military command tasked with protecting the nation is largely undefined.

The Secretary of Defense “has statutory roles and authorities under Title 10 and under Title 50.” Title 10 and Title 50 do not operate exclusively of each other, and it has long been thought the way in which an operation is reported can dictate the level of Congressional oversight. Hence, previous jurisdictional conflicts between operations conducted under Title 10 and operations conducted under Title 50 make current lawmakers wary of giving military commands, such as USCYBERCOM, jurisdiction to conduct intelligence activities, especially if those intelligence activities are domestic.

IV. PROPOSED SOLUTION AND SUPPORTING ANALYSIS

A. The Proper Role of U.S. Military Forces and Intelligence Agencies in Cyberspace

Generally, USCYBERCOM’s jurisdiction would not extend beyond that of DoD and an existing forces command because it falls under DoD jurisdiction. Yet, because cyberspace is an area unlike any other domain where war is

112. For example, JP 2-0, Joint Intelligence, provides “the current guidance for conducting joint and multinational intelligence activities across the range of military operations.” Joint Chiefs of Staff, Joint Pub. 2.0: Joint Intelligence (2007), available at http://www.fas.org/irp/doddir/dod/jp2_0.pdf.

113. See Wall, supra note 9, at 91 (“While ordinary Americans in the heartland may care only that U.S. national security objectives are effectively accomplished, military and intelligence bureaucrats and their Congressional overseers remain obsessed with who actually does the mission.”).

114. Wall, supra note 9, at 100.

115. See Wall, supra note 9, at 100 (“There is no rigid separation between Title 10 and Title 50.”). For example, “[t]itle 10 includes authority for the Secretary of Defense to engage in both intelligence activities and military operations.” Id. at 103.

116. When discussing “the division between Title 10 and Title 50 operations” in cyber law and cyber warfare, John Rizzo, former general counsel of the CIA, noted that the description of cyber-operations, whether under Title 10, “being undertaken by the Pentagon,” or under Title 50, “being covert action operations conducted by the CIA,” “will dictate how they are reviewed and approved in the executive branch, and how they will be reported to Congress, and how Congress will oversee these activities.” Wall, supra note 9, at 108 n.77, 109.

117. For example, one blogger believes “DoD is deliberately trying to avoid reporting information on cyberwarfare programs to Congress.” Wall, supra note 9, 108 n.77 (citing Hiding our Cyberwar from Congress, EMPTYWHEEL (Jan. 14, 2011) http://emptywheel.firedoglake.com/2011/01/14/hiding-our-cyberwar-from-congress).
traditionally waged,\textsuperscript{118} USCYBERCOM must operate more freely than traditional military commands.\textsuperscript{119} In order to protect its domain and effectively operate in its AOR, which seemingly has no boundaries, USCYBERCOM must be responsible for coordinating national cyber power, intelligence agencies, and the private sector in both offensive and defensive cyber capabilities.\textsuperscript{120} In order to effectively do this, USCYBERCOM must share intelligence-gathering activities with federal agencies and the private sector, given the unique nature of cyberspace and the traditional military command structure’s inadequacy in effectively protecting this domain.\textsuperscript{121} Providentially, USCYBERCOM’s commander advocated various relationships across departments to further national security interests.\textsuperscript{122}

In traditional military combatant commands, the commanders work closely with the Central Intelligence Agency (CIA) in executing military combat operations. However, the CIA is prohibited from collecting intelligence regarding “U.S. Persons.”\textsuperscript{123} While Americans tend to distrust the U.S. National Security Agency (NSA) and the intelligence agencies,\textsuperscript{124} they protect the military’s image,
especially those who serve the nation. Overall, the existing structure between intelligence agencies and military commands is inadequate for the demands of cyberspace because there is not adequate freedom to share information. For example, “[t]he NSA is not authorized to assist operations of private sector critical infrastructure systems directly.” Similarly, “DoD has no authority to enforce military doctrines outside of the Department.” Thus, in order to capably secure cyberspace, USCYBERCOM must have the authority to call upon other federal agencies and the private sector.

Undeniably, there is a need for DoD to share information with other government organizations and the private sector. It is a daunting task to ensure that Americans’ privacy rights and civil liberties are protected, while also safeguarding economic and national security. Understanding this, DHS used its Cyberspace Policy Review to emphasize the need to “realize the full potential of the information technology revolution” while also recognizing the “great risks [that] threaten nations, private enterprises, and individual rights.” Yet, DHS denoted its role in conjunction with “a wide array of federal departments and agencies, many with overlapping authorities and none with sufficient decision authority to direct actions that deal with often conflicting issues in a consistent way.” Clearly, the number of players involved in securing cyberspace highlights the difficulty for USCYBERCOM to be effective without a robust directive that enables it to act decisively and unilaterally. There is a discernible disparity between operational capabilities in cyberspace and “the governing laws and policies.”

comes to the controversial programs and unveiled steps to increase transparency and accountability at the NSA.”).  
125. See Wall, supra note 9, at 141 (“Military leaders must vigilantly ensure the U.S. military retains the respect and admiration of the American public and executive branch bureaucrats will always seek to protect their domains.”).
126. Greer, supra note 124, at 140-41.
127. Young, supra note 106, at 175.
128. Gregory T. Nojeim, Cybersecurity: Ideas Whose Time Has Not Come-and Shouldn’t, 8 I/S: J.L. & POL’Y FOR INFO. SOC’Y 413, 431 (2012) (“There is a well-founded belief that information sharing is an important aspect of any cybersecurity program.”). This undercuts the common misconception that there must be “a strict separation between intelligence activities and military operations even when no such separation is legally required.” Wall, supra note 9, at 122.
129. See Greer, supra note 124, at 139.
131. Policy Review, supra note 130. See also Mark D. Young, United States Government Cybersecurity Relationships, 8 I/S: J. L. & POL’Y FOR INFO. SOC’Y 281, 282 (2012) (“Strong operational relationships are necessary for the management and protection of federal networks because no single federal branch, department, or agency has the authority or resources to operate and defend the interconnected systems needed to perform government functions.”).
132. Advance Questions, supra note 89.
cyber security responsibilities.\textsuperscript{133} Because USCYBERCOM possesses more cyber capabilities than DHS, it should have direct intelligence-gathering jurisdiction, without being forced to act as DHS’s support command.

Cyber warfare can include domestic acts and domestic actors; thus, USCYBERCOM should serve at the forefront of defending the nation in a real-time capacity, rather than its current restriction to operating only on DoD networks.\textsuperscript{134} Yet, the American people will distrust an organization with intelligence-gathering capabilities that has unilateral authority.\textsuperscript{135} The geographic boundaries that previously guided the roles and responsibilities of DHS and DoD are less clear in cyberspace.\textsuperscript{136} Historically, the NSA had a bifurcated structure that handled its foreign intelligence collection separately from its domestic activities.\textsuperscript{137} This structure made sense, especially given the prohibitions against gathering intelligence on U.S. citizens regardless of their worldwide location.\textsuperscript{138} With cyberspace, however, the distinction between “foreign” intelligence and “domestic” intelligence is less clear, creating the need for legal guidance that will be effective, while also protecting privacy rights and civil liberties.\textsuperscript{139} For example, information that non-American citizens store over “cloud” computing services based out of the United States “can be spied upon routinely without their knowledge by U.S. authorities” under FISA.\textsuperscript{140} Overall, because domestic law enforcement and intelligence agencies can lawfully support combatant


\textsuperscript{134} See Young, supra note 106, at 176.

\textsuperscript{135} To illustrate, confidence in the NSA to adhere to requirements of transparency was “undermined by its conduct in the Terrorist Surveillance Program (TSP) for approximately five years after the September 11, 2001 terrorist attacks.” Nojeim, supra note 128, at 423. This program conducted “secret surveillance in the U.S” and is now “widely thought to have been both unconstitutional and unlawful warrantless surveillance under the Foreign Intelligence Surveillance Act (FISA).” Id. (citing 50 U.S.C. §§ 1801-1871 (2006)).

\textsuperscript{136} See Greer, supra note 124, at 139 (“It is no longer appropriate to think in terms of geographic boundaries between ‘foreign’ and ‘domestic’ activities because these concepts lose their meaning in cyberspace.”).

\textsuperscript{137} Greer, supra note 124, at 140. Additionally, “[t]he NSA’s foreign and domestic arenas traditionally differed in many respects, including staff, oversight and compliance requirements, budgets, and authorities.” Id.

\textsuperscript{138} For example, “restrictions…were developed to protect the privacy rights of U.S. persons whose communications were intentionally targeted to obtain foreign intelligence.” Greer, supra note 124, at 140. These actions required a court order under the FISA. Id. (citing 50 U.S.C. § 1801 (2006)).

\textsuperscript{139} Greer, supra note 124, at 140 (“The task is how to expand the sharing of cybersecurity information when intelligence agencies are involved while protecting privacy rights and civil liberties.”).

commands through joint intelligence efforts, USCYBERCOM will require a robust connection to DHS and, more specifically, the Federal Bureau of Investigation (FBI).¹⁴¹

B. Involving Concerns of Private-Sector Vulnerabilities

Currently, any participation by private sector companies to share information with the government is voluntary.¹⁴² Additionally, the division of cyber security capabilities between civilian agencies and DoD is immensely disproportional.¹⁴³ As structured, DHS is responsible for both cyber security in civilian government systems and “working with the private sector to secure networks associated with critical infrastructure.”¹⁴⁴ Unfortunately, this monumental task has largely been unfulfilled to the extent proposed by the Homeland Security Act of 2002.¹⁴⁵ Conversely, DoD, through USCYBERCOM, is creating “a complex threat environment with many actors and interconnected networks.”¹⁴⁶ Thus, DoD should work with the NSA, but should lead the government’s cyber power through USCYBERCOM and interact directly with the private sector to strengthen the nation’s cyber security.

While some scholars believe that requiring private sector corporations to share information with the government would lead to “less corporate and public participation” because of decreased transparency with the public,¹⁴⁷ the ability for a single command to interact with the private sector, coupled with strengthened protections through Freedom of Information Act (FOIA) mandates, would actually increase participation and ultimately strengthen U.S. cyber capabilities.

The main arguments against private information-sharing with government cyber operations include “[c]oncerns over privacy, network service availability,  

¹⁴¹ “The FBI has primary responsibility for [counterintelligence] CI and counterterrorism operations conducted in the United States. The FBI shares law enforcement and CI information with appropriate DOD entities and combatant commands.” Joint Chiefs of Staff, Joint Pub. 2.0: Joint Intelligence (2007), available at http://www.fas.org/irp/doddir/dod/jp2_0.pdf.


¹⁴³ Young, supra note 106, at 173 (“The capacity of civilian agencies is too small, while the Defense Department’s role in network operations is too large.”).

¹⁴⁴ Nojeim, supra note 128, at 423.


¹⁴⁶ Nojeim, supra note 128, at 421-22.

¹⁴⁷ Nojeim, supra note 128, at 422.
criminal and civil liability risks, and intellectual property protections.” In order to make USCYBERCOM effective at working with private corporations, Congress must legislate to protect “against privacy lawsuits from customers and other potential liabilities.” Specifically, Congress must expand the exemptions under FOIA so that the private sector will not be exposed to substantial liability because of requirements to share information with DoD and other federal agencies.

Currently, private companies are concerned about the potential exposure to civil liability under current law if they are forced to release customer information. These privacy and business concerns created much of the disagreement that led to Congress’s inability to agree on legislation to facilitate interagency efforts between DoD and DHS. Yet, statutory guidance will be necessary to garner the private sector’s support in sharing information with government agencies. Under federal law, agencies are required to make information available to the public unless that information falls within a certain exemption. By extension, any information that a private sector firm would provide to the government could be released to the public. The U.S. Supreme Court has consistently upheld FOIA mandates, requiring “broad disclosure of Government records.” Congress created nine exemptions to FOIA because “public disclosure is not always in the public interest.” Nonetheless, opening up private sector companies to the possibility of civil liability for disclosing certain information will curtail any efforts to strengthen the federal government’s

---

148. Young, supra note 106, at 190. Additionally, Defense Secretary Chuck Hagel cited the private sector concerns that are mounting as a result of the interagency efforts between DoD and DHS. See Parrish, supra note 133.


150. See Young, supra note 131, at 321.

151. Parrish, supra note 133.

152. As USCYBERCOM’s commander argued that defending against cyber attacks in real time “will require legislation removing barriers to private-to-public sharing of attacks and intrusions into private-sector networks.” Marshall, Jr., supra note 142.


155. FOIA has nine exemptions that shield agencies from releasing documents to the public. See Freedom of Information Act Exemptions, U.S. Securities and Exchange Comm’n (Dec. 1, 1999), http://www.sec.gov/foia/nfoia.htm (listing the nine exemptions, which includes “[t]hose documents properly classified as secret in the interest of national defense or foreign policy”).

156. Young, supra note 131, at 321 (The information provided by the private-sector firm could still be protected under a FOIA exemption, such as the exemption for national security).


ability to protect cyberspace. Thus, Congress should strengthen FOIA to protect the private sector from liability so that the appropriate level of information sharing can take place. At the same time, Congress must also account for the political distrust surrounding the NSA’s wide discretion in gaining access to information on the sole basis of U.S. foreign policy.

V. CONCLUSION

The threat of cyber warfare is becoming a contemporary norm with regard to U.S. military commands. As the U.S. relies more heavily on cyber infrastructure to wage attacks, it will be even more important to secure military networks against unlawful infiltration. As a domain unlike any of the physical realms in which combat operations have traditionally taken place, cyberspace requires a new operational structure that includes a robust collaboration with national intelligence agencies and U.S. private sector firms. Moreover, USCYBERCOM is best equipped to defend the nation’s cyberspace, and should be given the lead on this task. Accordingly, USCYBERCOM should shoulder the responsibility of securing cyberspace because of its classification as a war-fighting domain. In order to effectively do this, USCYBERCOM must be able to call upon other government agencies and the private sector. Even though this may result in some non-traditional interactions with Americans’ privacy and private corporations’ private information, it is the only way for the U.S. to secure cyberspace and for USCYBERCOM to effectively operate as a combatant command.

159. Young, supra note 131, at 323 (discussing “the private sector’s limited inclination to share with government due to its proprietary concerns and liability issues”).
160. See Hastings, supra note 140.
161. See Roulo, supra note 48 (“Army Gen. Martin E. Dempsey . . . anticipates a day when operations in cyberspace become a dominant factor in military operations.”).
162. See Def’t of Def. Strategy for Operating in Cyberspace, supra note 1, at 1 (“DoD operates over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe.”).
I. INTRODUCTION

In May 2007, Estonia suffered a massive cyber-attack on both its government and civilian networks, “[h]itting the websites of banks, ministries, newspapers, and broadcasters,” and shutting down communications so that Estonia could not communicate with the outside world.1 The attack left Estonians unable to call for emergency services, and it also left many government and non-government entities unable to access the Internet for nearly two weeks.2 The overall damage from the cyber-attack was estimated to be roughly 5 percent of the overall economic activity of the country.3 This damage was not surprising for a country considered to be the most wired in Europe as roughly 90 percent of banking transactions and online tax payments, and roughly 5 percent of voting for national elections is conducted online.4 While no state has claimed responsibility for the attack, a non-state actor associated with the Kremlin-backed youth movement accepted responsibility without any state involvement.5

Although the Estonian story is real, imagine, hypothetically, that members of Al Qaeda launched a cyber-attack against the air traffic control systems of the John F. Kennedy International airport in New York, shutting down any communication between air traffic control and the planes landing and taking off. As a result, the lack of communication causes several planes to crash, causing death and destruction to several hundred affected.

The types of options available to both the Estonian and U.S. governments depend on how international laws of war apply to cyber-attacks. Specifically, two issues must be addressed. Under international laws of war, a state that suffers an “armed attack” can assert a right of self-defense against the actor.6 Thus, the first question is whether a cyber-attack can ever constitute an “armed attack” under the U.N. Charter. Yet, for state actors like the Estonian government, another legal question must be addressed when attacks the cyber-

3. See id. at 201.
attacks are claimed by non-state actors. Hence, the second question is whether a non-state actor can ever commit an “armed attack” under the U.N. Charter. However, currently, both issues are unresolved and uncertain.

With respect to the first issue, most scholars opine that a cyber-attack constitutes an “armed attack” only if the attack causes death and destruction to property. Under this approach, the cyber-attacks against Estonian would fail to be an “armed attack” because the damage did not result in death or destruction. In the hypothetical situation, the cyber-attack against the U.S. would constitute an “armed attack.”

With respect to the second issue, a recent advisory opinion from the International Court of Justice (“ICJ”) suggests that an armed attack can only be committed by state actors. If so, then both the Estonian and U.S. governments are left unable to take advantage of self-defense under international laws of war, creating a potential vacuum for non-state actors to attack and hide behind the veil of the state in which they are located. Given this ever-growing threat, the U.S. cannot afford to leave these issues unresolved. Every fabric of modern American life has become “intertwined with, and dependent on” the Internet and cyberspace, making the U.S. the most vulnerable state to a cyber-attack.

Compounding the vulnerabilities of the U.S. is the grave threat of a cyber-attack. Former U.S. Secretary of Defense, Leon Panetta, has stated that “[a] cyber attack perpetrated by nation states [or] violent extremists groups could be as destructive as the terrorist attack on 9/11.” Moreover, a recent U.N. Panel recognized that the threat of a cyber-attack is “among the most serious challenges of the twenty-first century.”

Like other weapons, the potential threat from a cyber-attack is devastating; but, unlike other weapons, the cost to launch a cyber-attack is affordable to most nations. “[A] study by the RAND corporation found the costs of developing the cyber weapons needed for conducting cyber warfare to be extremely modest and within financial reach for nearly every state.”

7. Li, supra note 2, at 187.
8. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, P 139 (July 9) [hereinafter Wall].
13. Id.
Therefore, given its vulnerabilities and the ease with which its enemies can obtain cyber weapons, the U.S. should be a leader in advocating that existing international laws of war apply to a cyber-attack launched by both a state and non-state actor. To support this position, this Note proceeds in five parts. Part II provides background information on cyber-attacks and cyber warfare. It also highlights a number of recent cyber-attacks by state and non-state actors. Part III offers historical analysis on current international laws of war with emphasis on the U.N. Charter. Part IV highlights the current challenges and current recommendations on whether international laws of war apply to cyber-attacks. This part outlines a number of popular approaches to the question of whether a cyber-attack constitutes an “armed attack,” and whether a non-state actor can commit it. Part V proposes the way forward in addressing the current challenges. Specifically, this Note proposes that a cyber-attack can constitute an “armed attack” under a non-kinetic effects-based approach. Also, this Note argues that non-state actors can commit an “armed attack.” To achieve both, this Note proposes defining cyberspace as a hybrid form of common property. Each state should be able to access the Internet, but each state should be responsible for preventing cyber-attacks from being launched within its territory.

II. CYBER WARFARE: THE NEW NATIONAL SECURITY THREAT

Before attempting to apply international law to cyber-attacks, one must first define cyber-attack and cyber warfare. A definition too narrow might allow many attacks to escape international war law, while a definition too broad may not serve the U.S. national interest by encompassing a number of military tactics that need to be distinguished, such as espionage. For example, the world has recently learned that the U.S. Government’s National Security Agency (“NSA”) has obtained personal phone and Internet-usage data from all U.S. citizens. If the U.S. government continues to engage in such conduct domestically and expands it abroad, whether this constitutes a cyber-attack is critical for modern U.S. intelligence.

Thus, at a time when no nation is free from the threat of a cyber-attack, the need for a workable definition is critical. Yet, to date, no internationally-accepted definition exists. Nevertheless, in general, three terms should be defined: cyberspace, cyber warfare, and cyber-attacks.

A. What is a cyber-attack?

1. Cyberspace

Cyberspace is the domain in which the Internet and cyber warfare occur. This is a domain “where information is created, stored, modified, and exploited via interconnected networks.” The Department of Defense (“DOD”) defines cyberspace as “[a] global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the [i]nternet, telecommunications networks, computer systems, and embedded processors and controllers.” Others have defined it as “the environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the World Wide Web.” Also, the National Military Strategy for Cyberspace Operations defines cyberspace as “[a] domain characterized by the use of [computers and other electronic devices] to store, modify, and exchange data via networked systems and associated physical infrastructures.”

While these definitions are similar, they also highlight the complexity among the international community on the scope of cyberspace. Even adopting the most restrictive definition encompasses the internet, telecommunication infrastructure, and computer networks. This commentary is designed to offer a range of definitions for cyberspace, and for purposes of this Note and cyber-attacks, any of them will suffice. Going forward, however, the DOD offers the most effective definition of cyberspace because it is the most comprehensive.

2. Cyber Warfare

Like the term cyberspace, “cyber warfare” has no widely accepted definition. Unlike with cyberspace, where most definitions encompass the appropriate scope, a state defines “cyber warfare” is critically important. Some have defined cyber warfare as an “an attack by one hostile nation against the computers or networks of another to cause disruption or damage.”

---

However, this definition is too narrow because it fails to consider the modern-day impact of non-state actors. If cyber warfare is limited to nation-states, then the activities of terrorist organizations and other non-state actors necessarily fall outside the definition and therefore outside the international laws of war. Consequently, under this restrictive definition, a victim state would not be able to assert a right of self-defense against a non-state actor because a non-state actor cannot engage in cyber warfare.

In contrast, the DOD defines cyber operations as “[t]he employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.”

Interestingly, the DOD previously defined it as “[t]he employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.” Here, although the DOD eliminated the term “effects,” it also eliminated the term “military” as a modifying objective. Thus, the DOD has moved toward a more expansive definition of cyber operations, or cyber warfare. The new definition is broad enough to include non-state actors that are not designed to achieve merely military objectives, but also economic strangulation, society disruption and chaos, as well as other major challenges that come with cyber warfare.

The international community should adopt the DOD’s modernized definition of cyber warfare. Any definition that limits cyber warfare to military objectives or nation-states overlooks the reality that a cyber-attack launched by a non-state actor for a non-military objective poses equal threat to our national security, such as Al Qaeda and other criminal or terrorist networks.

3. Cyber-Attack

In addition to the importance of defining cyber warfare, how a state defines a cyber-attack is also critical. Predictably, to date, no uniform definition exists. The U.S. Army defines a cyber-attack as “[t]he premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or to further social, ideological, religious, political or similar objectives.” Although this definition focuses on the physical disruption, it is a good starting point. Here, the focus is on disruption of computers or

---

23. JP 1 *supra* note 18, at 64.
24. Joint Chiefs of Staff, Joint Publication 1-02, Dep’t of Def. Dict. of Military & Assoc’d Terms, at 141 (12 Apr. 2001)
networks. Presumably, this would include the Internet and cyberspace, but it is not clear from the face of the definition.

Additionally, Michael Hayden, former director of the NSA and the Central Intelligence Agency ("CIA"), defines cyber-attack as a "deliberate attempt to disable or destroy another country’s computer networks." In contrast, Matthew Waxman has defined cyber-attacks as "efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them." The second definition expands the activities to more than a disruption, and it unequivocally includes both the physical computers and the systems within them. Therefore, this note adopts Matthew Waxman’s definition.

Under this definition, the U.S. government’s recent efforts to obtain personal information through the NSA would not constitute a cyber-attack. To procure this information, the NSA has requested phone records and other personal information from Google, Facebook, and other Internet companies regarding U.S. citizens. Although constitutional and other legal questions surface regarding the NSA’s methods of collection, these efforts and other international information-gathering efforts merely obtain personal information about private citizens. To date, no news reports exist to show that the NSA has disrupted or destroyed any computer networks or other systems to obtain this information. Rather, the sheer invisible nature of the NSA’s activity has contributed, in part, to the national reaction. However, a narrow definition of a cyber-attack would subject the U.S. government’s self-proclaimed terrorist deterrence program to be an attack on its own citizens.

A final point must be made regarding the distinction between cyber-attacks and cyber-crimes. A cyber-attack can range from “malicious hacking and defacement of websites to large-scale destruction of the military or civilian infrastructures that rely on those networks.” Cyber-crimes, “like fraud or posting obscene and offensive content on the Internet, are governed by national criminal laws.”

---

31. Id.
B. Types of weapons used in a cyber-attack

Roughly 140 nations have active cyber-weapons-development programs.\textsuperscript{32} Within these programs, cyber weapons can come in a variety of forms. The more popular types of cyber-attacks are: Denial of Service ("DoS") attacks, Distributed denial of service ("DDoS") attacks, malicious programs, and logic bomb.

1. DoS and DDoS attacks

As the most prevalent cyber weapon, DoS attacks are an attempt "to prevent legitimate users of a service from using that service."\textsuperscript{33} Under a DoS attack, an attacker will flood a network with excessive information and data requests beyond what it can handle to a level that causes the network to slow or stop.\textsuperscript{34} The result is the inability of a user to access "email, websites, online accounts, or any other service that relies on the affected computer" or network.\textsuperscript{35}

On the other hand, a DDoS attack is like the "meaner cousin" of the DoS.\textsuperscript{36} A DDoS attack assails multiple computers that are "preinfected with a virus that hijacks the computer to attack Web sites, making it exponentially more powerful than a standard DoS attack."\textsuperscript{37} Thus, an attacker may take control of multiple computers and send the attack to another set of computers that will eventually over-flood a network.\textsuperscript{38} For example, in July 2009, "a number of government and commercial websites in the United States and South Korea were shut down by a DDOS attack."\textsuperscript{39}

2. Malicious programs: viruses and worms

Malicious programs enable the attacker to disrupt the normal functions of a cyber network by infecting the network or taking control over it.\textsuperscript{40} Malicious programs can take effect immediately, or they can be time delayed.\textsuperscript{41} For example, an attacker could invade a network like air traffic control systems on Monday, then either disrupt the functions immediately or delay the disruption for Tuesday.

\textsuperscript{32} See Schaap, supra note 12, at 135.
\textsuperscript{33} DeLuca, supra note 30 at 282-83.
\textsuperscript{34} Id.
\textsuperscript{35} Id. at 283.
\textsuperscript{37} Id.
\textsuperscript{38} See DeLuca, supra note 30, at 283.
\textsuperscript{39} Hathaway, supra note 27, at 838.
\textsuperscript{40} See Schaap, supra note 12 at 135.
\textsuperscript{41} Id.
A virus is a defective computer code written to attach to a network or program without the user’s knowledge. A virus is a defective computer code written to attach to a network or program without the user’s knowledge. Although it must attach itself to a computer network, the most attractive feature of the virus is its ability to replicate itself and spread from computer to computer after its introduction to the initial target. The damage can be significant. In 2000, the “I Love You” virus, released in the spring of 2000, caused an estimated $6.7 billion in damage.

Similarly, a worm spreads computer-to-computer, but it does so without the help of a user. A worm is an independent program” that eats away at a network’s data or function capabilities. A worm does not need to attach itself to any program or network. Generally, “[d]ue to the copying nature of a worm and its capability to travel across networks, the end result in most cases is that the worm consumes too much system memory or network bandwidth, causing web servers, network servers, and individual computers to stop responding.”

3. Logic bombs

A logic bomb is like an intelligent computer bomb. The logic bomb sits dormant in a network until a set of pre-determined conditions are met, at which point the “program executes its malicious function.” Because it is not readily detectable due to its dormant nature, the effects can be more devastating. During the Cold War, the U.S. government used this weapon to destroy a Soviet natural gas pipeline.

Other cyber weapons include Internet Protocol (“IP”) spoofing and Trojan horse. IP spoofing involves trickery whereby a user who enters a legitimate web address is re-directed to a fraudulent web site created by a hacker. If the deceived user interacts with the fraudulent website, the attacker can gain access to the user’s sensitive and confidential information. A Trojan horse is a “malicious software that fools a computer user into thinking that it will perform a wanted function but instead gives unauthorized access to the infected machine to a third party.”

42. See DeLuca, supra note 30, at 282.
43. Id.
44. Id. (citing Jason Barkham, Information Warfare And International Law on the Use of Force, 34 N.Y.U. J. INT’L L. & POL. 57, 62 (2001)).
45. See Schaap, supra note 12, at 136.
46. DeLuca, supra note 30, at 283.
47. Id. at 284.
49. McGavran, supra note 36, at 263.
50. Id.
51. Id.
52. See generally Schaap, supra note 12, at 137-38 (describing both IP Spoofing and Trojan horses as cyber warfare weapons).
53. Id. at 137.
54. Id.
55. McGavran, supra note 36, at 263.
C. Examples of cyber-attacks

1. Less-known cyber-attacks

Although in use since the Cold War, cyber-attacks gained a lot of traction in the 1990s, but these early attacks focused on collecting information, not disrupting or destroying computer systems. In 1998, over 500 U.S. computer systems were attacked, including military, commercial, and educational systems. These attacks, later called Solar Sunrise, were designed to obtain sensitive information rather than disrupt or destroy systems. Although the U.S. believed Iraq was behind the attacks, an investigation confirmed that teenagers from Israel and California created them.

In 1999, the United States planned to “feed false target data into the Serbian air defense command network, inhibiting Serbia’s ability to target NATO aircraft.” This attack was designed to disrupt Serbia’s air defense and exploit Serbia’s increasing reliance upon computer networks. However, the plan was abandoned because NATO feared it “put civilian targets at risk, with the air-defense network possibly confusing relief planes or commercial aircraft for military targets.”

More recently, the Israeli Air Force launched a cyber attack in 2007 against the Syrian air-defense system, allowing the Israeli planes to fly undetected in order to strike Syria’s nuclear facility. In 2009, “a number of government and commercial websites in the United States and South Korea were shut down by a DDOS attack.” Although the commercial and government entities felt the impact of the attack, the source was not readily known.

2. Estonia and Georgia

Gaining the most scholarly and media attention, the recent cyber-attacks against Estonia and Georgia represent the potential serious consequences of a cyber war.

56. See, e.g., id. at 263 (detailing the use of a cyber attack by the United States during the Cold War).
57. See Huntley, supra note 9, at 7-8 (“Those responsible for these intrusions gained access to DoD computer systems around the world, left a program that would collect data from the system, and then later returned to retrieve that data.”).
58. Id. at 8.
59. Id.
60. Id.
61. Hathaway, supra note 27, at 838.
62. Id.
64. Hathaway, supra note 27, at 838.
65. Id.
66. See id. (“There remain questions about where the attack originated.”).
In 2007, “a series of DoS attacks” were launched against websites in Estonia, including the website of the president, parliament, and political parties. A Defense Ministry spokesman stated that some websites that receive 1,000 visits per day were receiving 2,000 visits per second.

As one of the most wired country in Europe, the attacks caused significant distress on the country of distressed Estonia. For example, “[b]anks, news agencies, telecom companies, and government ministries suffered loss of Internet access over the next two weeks.” The “attacks shut down several government Websites,” and emergency lines for fire and ambulance remained offline for an hour. Consequently, “the people of Estonia quickly turned to the streets in riot, leaving at least one person dead and 150 people injured.” Altogether, the damage totaled approximately 5 percent of Estonia’s overall economic activity.

In 2008, Russia launched a war with Georgia over disputed territory, dropping physical bombs throughout Georgia’s capital. A few months before the conflict, Georgia suffered a cyber-attack, bringing down Georgian servers and hurting communication throughout the country. Georgia was the victim “of DoS attacks, Web site hijacking, and the defacing of Georgian news and government Web sites to include propaganda.” The result was “the country found itself unable to communicate with the outside world over the Internet as Russian forces invaded South Ossetia.” Later, the two countries agreed to a cease-fire, and although the physical war had ceased, Georgia’s Internet infrastructure and website-server communications remained largely inoperable.

In 2010, a computer worm called Stuxnet introduced cyber warfare to the conflicts in the Middle East. The computer malware was designed to target Iran’s nuclear program. Stuxnet infected Iranian nuclear facilities; eventually,
Iranian President Mahmoud Ahmadinejad confirmed that Stuxnet set back the Iranian nuclear program.\textsuperscript{83} Although Stuxnet’s origin is unknown, strong evidence points to both the United States and Israel.\textsuperscript{84} “If true, [it] represents one of the first excursions of governments into the murky waters of cyber war.”\textsuperscript{85}

\textbf{D. States’ developments of cyber warfare strategies}

NATO’s Chief of Cyber Defense has indicated his belief that cyber warfare is just as much a national security threat as a missile attack.\textsuperscript{86} The issue is compounded by the reality that ninety percent of the military voice and Internet communications travel over the same private service networks that serve private homes and businesses.\textsuperscript{87} Given the serious consequences of a cyber-attack, many states have begun to develop cyber warfare strategies to address this modern-day warfare.

1. The U.S.

In 2002, President Bush signed the National Security Presidential Directive 16, triggering the first move towards a cyber warfare strategy.\textsuperscript{88} The Directive instructed the government to establish a plan for the use of cyber warfare as a weapon.\textsuperscript{89} Additionally, in 2003, a White House document made “clear that the U.S. government reserves the right to respond [to a cyber attack] ‘in an appropriate manner.’”\textsuperscript{90} In 2005, the Air Force expanded its mission statement to reflect cyberspace.\textsuperscript{91} By 2006, the Department of Defense’s policy stated that U.S. should strive to reach “strategic dominance in network technologies” and “information superiority.”\textsuperscript{92}

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{83} Cammack, supra note 82, at 317.
\item \textsuperscript{84} See Richmond, supra note 81, at 845.
\item \textsuperscript{85} Id.
\item \textsuperscript{86} See Schaap, supra note 12, at 123.
\item \textsuperscript{87} Kirsch, supra note 74, at 644 n.124.
\item \textsuperscript{88} Natasha Solce, \textit{The Battlefield of Cyberspace: The Inevitable New Military Branch—the Cyber Force}, 18 ALB. L.J. SCI. & TECH. 293, 302 (2008); Schaap, supra note 12, at 128.
\item \textsuperscript{89} Schaap, supra note 85, at 128.
\item \textsuperscript{90} Id. (quoting Clay Wilson, \textit{CONG. RESEARCH SERV.}, RL32114, Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress 15 (2003)).
\item \textsuperscript{91} Id. at 131.
\item \textsuperscript{92} Id. at 128 (quoting U.S. DEP’T OF DEF., NO. O-3600.1, INFORMATION OPERATIONS 2 (2006), available at http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-022.pdf).
\end{itemize}
\end{footnotesize}
2. Other States

China’s cyber warfare doctrine is designed to reach “global electronic dominance” by 2050. In 1999, the official media outlet for the People’s Liberation Army of the People’s Republic of China stated “Internet warfare is of equal significant to land, sea, and air power and requires its own military branch.” To that end, recent reports from the U.S. government show that China has prepared units to launch attacks against enemy computer networks. Similarly, Russia’s armed forces have developed a cyber warfare doctrine that “would disrupt financial markets and military and civilian communications capabilities as well as other parts of the enemy’s critical infrastructure prior to the initiation of traditional military operations.”

In 1998, North Korea created a military unit to focus solely on cyber warfare. Its progress has been so rapid that it tested its first cyber weapon in 2007, and as a result of that test, a U.N. Security Council Resolution banned sales of mainframe computers and laptop PCs to North Korea.

III. INTERNATIONAL LAWS OF WAR

War is chaotic, but within its seemingly chaotic character, war is governed within an organized legal framework. Serving as this framework, the international laws of war are split into two divisions: *Jus ad bellum* and *jus in bello*. “*Jus ad bellum* is the body of law that applies prior to a conflict . . . while *jus in bello* governs behavior during a conflict.” The international community refers to *jus in bello* as “laws of war, laws of armed conflict (“LOAC”), or international humanitarian law.” The primary focus of this note is on the LOAC. To better understand the international laws of war, a brief historical perspective is helpful.

93. Schaap, supra note 12, at 132.
95. See Schaap, supra note 12, at 132-33.
96. Id. at 133.
97. Id.
98. Id.
99. Richmond, supra note 81, at 8634.
A. History of laws of war

Many “legal scholars believe that the Treaty of Westphalia created the modern nation state in 1648.”

Before the Treaty of Westphalia, states evaluated whether to wage war based, in part, upon decisions of justness and morality. After passage of the Treaty of Westphalia, however, the evaluation of whether to wage war increasingly became one of legal analysis.

As the late nineteenth century arrived, advancements in technology led to an atrocious American Civil War, and soon after, the world began to revisit war through the lens of morality. Accordingly, in the late 1800s, the LOAC began in an effort to help protect soldiers wounded in battle and restore the sense of morality in war.

In 1907, a peace conference led to the passage of the Hague Conventions to govern the laws of war. Establishing the foundation for all war laws, the Hague Convention’s basic premise is “the right to take action to injure an enemy in war is not unlimited.” Later, however, the basic concepts of the Hague Convention were challenged by two World Wars that lead to death and destruction on a scale unmatched in world history.

Consequently, in 1949, the precepts of the Hague Convention were expanded with the passage of the four Geneva Conventions. The Geneva Conventions replaced the word “war” with “armed conflict” in an effort to “widen humanitarian protections to state actions that might not be technically defined as acts of war.” But, the Geneva Conventions were not fully completed until passage of Protocol I and II in 1977.

Today, the LOAC is governed, in part, by these conventions and protocols. However, it is also governed by customs, expanding the number of states within reach of the LOAC to include those that have not formally adopted the Conventions. Although a large portion of the LOAC is composed of the Conventions and customary laws, a primary source of war law is the U.N.

104. Id.
105. Id.
106. Id.
107. See Richmond, supra note 81, at 867.
108. See Cohen, supra note 102, at 395.
109. Id.
110. See Stevens, supra note 103, at 669-70.
111. Cohen, supra note 102, at 395.
112. Id.
113. Id.
114. Id. (citing International Committee of the Red Cross (2009)) (“War is governed by a set of international rules established by treaty or custom to ensure that the humanitarian problems that arise as a result of armed conflict are either prevented from occurring or responded to. These rules are collectively known as the ‘law of armed conflict’”).
115. Id.
Even if another international agreement conflicts with the U.N. Charter, the member state must follow the U.N. Charter.

**B. U.N. Charter**

The U.N. Charter’s (“the Charter”) purpose is to “maintain international peace and security.” The Charter created the Statute of the International Court of Justice, and together with the Charter, they regulate international disputes. Under article 2(4) of the U.N. Charter, a member state is prohibited from engaging in “the threat or use of force.” Although the term “force” is the subject of scholarly debate, the prevailing thought is that it “does not apply to political, psychological, or economic coercion, such as trade sanctions or propaganda.” Moreover, based on the plain language of the Charter, article 2(4) applies to state actors only.

The prohibition on the “use of force” under article 2(4) is not absolute. The Charter includes two exceptions to the general prohibition on the use of force: (1) upon U.N. Security Council (“Council”) approval, and (2) when a state is asserting its right of self-defense under article 51. Under article 39, the Charter authorizes the Council to “determine the existence of any threat to the peace, breach of the peace, or act of aggression and [to] make recommendations, or decide what measures shall be taken . . . to maintain or restore international peace and security.” To ensure peace, the Council may authorize the use of armed force. Further discussion regarding this exception is beyond the scope of this note.

**C. Right of self-defense**

The second exception is a states’ right of self-defense under article 51 of the Charter. Article 51 of the Charter states that “[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council

---


117. Charter art 103.

118. See Stevens, *supra* note 103, at 671.


120. Li, *supra* note 2, at 184.

121. See U.N. Charter art. 2, para 4 (referring exclusively to “any state.”).

122. See id. at art. 39.

123. See id. at art. 51.

124. Id. at art. 39.

125. See id. at art. 42.

126. U.N. Charter art. 51.
has taken measures necessary to maintain international peace and security."\textsuperscript{127} Accordingly, a state that has been the victim of an "armed attack" ("victim state") can act in self-defense to protect itself before the Council acts.\textsuperscript{128}

Before a victim state can assert its right of self-defense, an "armed attack" must first occur.\textsuperscript{129} Legal scholars generally agree that the U.N. Charter’s plain language confirms that an "armed attack" under article 51 is narrower than the “use of force” under article 2(4).\textsuperscript{130} Further, the ICJ has stated that the right of self-defense is reserved for the “most grave forms of the use of force.”\textsuperscript{131} In clarifying the difference between the two, the ICJ has stated it is one of “scales and effects.”\textsuperscript{132}

Nevertheless, the larger question is whether a cyber-attack constitutes an “armed attack.” If it does, then a victim state can assert its right of self-defense by responding to a cyber-attack. If it does not, then the victim state cannot respond with force either physical or virtual. Moreover, given the silence in article 51 with respect to what parties can commit an “armed attack,”\textsuperscript{133} it raises questions about whether a non-state actor like a terrorist organization can commit one. These questions are unresolved among legal scholars.\textsuperscript{134} This note will thoroughly analyze the issue in section V.

\section*{D. Governing principles of self-defense}

Assuming an actor has committed an “armed attack” and the victim state seeks to assert its right of self-defense, the victim state is not free to respond in any manner it pleases. Rather, consistent with the idea of morality, the victim state must exercise its right of self-defense by following a set of guiding principles set forth in the LOAC: necessity and humanity, neutrality, distinction, and proportionality.\textsuperscript{135}

\subsection*{1. Necessity and humanity}

A victim state’s act of self-defense must be necessary, “leaving no choice of means, and no moment for deliberation,”\textsuperscript{136} and it must comply with the principle of humanity by not causing unnecessary suffering.\textsuperscript{137}

\begin{thebibliography}{99}
\bibitem{127} Id.
\bibitem{128} See id.
\bibitem{129} Id.
\bibitem{130} See Waxman, supra note 11, at 427.
\bibitem{131} Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 191 (June 27).
\bibitem{132} See id. at 202.
\bibitem{133} See Charter art 51.
\bibitem{134} Waxman, supra note 11, at 427.
\bibitem{136} Li, supra note 2, at 183.
\end{thebibliography}
Codified in Article 35 of the Additional Protocol I, the principle of necessity states that an actor cannot “employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering.”\textsuperscript{138} Under the principle of necessity, the question is whether the particular act of self-defense is necessary to achieve a particular military goal.\textsuperscript{139} For example, if Al Qaeda was using civilian telephone networks within Afghanistan to launch an attack against the U.S., the U.S. must analyze whether an attack against those telephone networks was necessary to suppress the attack or achieve any other goal of self-defense.

2. Distinction

The principle of distinction requires the victim state to distinguish between civilian objects and military objects.\textsuperscript{140} Civilians and civilian objects cannot be the targets of an act in self-defense, unless they participate in the hostilities.\textsuperscript{141} To ensure this principle is honored, the ICJ has opined that a state must “never use weapons that are incapable of distinguishing between civilian and military targets.”\textsuperscript{142}

Civilian objects, or objectives, “are all objects that are not military objects.”\textsuperscript{143} Accordingly, the best way to understand civilian objects is to understand military objects. Military objectives are objectives that by “their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.”\textsuperscript{144} Thus, any objective that makes an “effective contribution” to a military action constitutes a military objective.

It logically follows that, a civilian objective that makes an effective contribution to a military objective can also serve as a military objective.\textsuperscript{145}

\textsuperscript{137} Jensen, supra note 136, at 1165.
\textsuperscript{138} Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 35, para 2, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol I].
\textsuperscript{141} Id.
\textsuperscript{142} Id. (citing Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 257 (July 8)).
\textsuperscript{143} Protocol I, supra note 139, at art. 52, para 1.
\textsuperscript{144} Id. at para 2.
International law treats these civilian objects as dual objectives.\textsuperscript{146} For example, “a bridge that normally carries civilian traffic and would be considered a civilian object would become a military objective based on its location if it became the means for the enemy’s armed forces to move to the battle.”\textsuperscript{147} But, in the modern world, everything from telecommunications to economic targets, including banks, can be subsumed into a dual objective. Although beyond the scope of this article, the interconnectedness of the modern world likely demands world leaders to re-evaluate the definition of a dual objective before civilian objectives become illusory.

3. Proportionality

Although the principle of distinction prohibits an actor from targeting civilians and their objects, the law of war understands some proper attacks may incidentally impact civilian objects.\textsuperscript{148} To protect against this possibility, the attack must also comply with the principle of proportionality. The principle of proportionality applies only to civilians and civilian objects, including dual-use objects.\textsuperscript{149} The actor must “balance the potential death or injury to civilians, the damage to civilian property, and the military necessity of destroying that military target against the potential damage and destruction to civilians and civilian objects.”\textsuperscript{150}

Under Article 51 of the Additional Protocol I, an act is not proportional if it is “expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.”\textsuperscript{151} “Proportionality limits the amount of force that can be used to destroy a military objective to that which does not cause unnecessary collateral destruction of civilian property or unnecessary human suffering of civilians.”\textsuperscript{152}

Although this note discusses the principle of proportionality under section VI, the author finds it helpful to point out that cyber warfare arguably favors better compliance with the principle of proportionality. In the past, “physical destruction may have been necessary to neutralize a target’s contribution to the enemy’s efforts.”\textsuperscript{153} Now, in launching a cyber-attack, a victim state can launch
a cyber-attack to simply “turn off” the enemy’s efforts. In explaining this phenomenon, Major Eric Talbot Jensen provides a few examples: “[f]or instance, rather than bombing an airfield, air traffic control can be interrupted. The same is true of power production and distribution systems, communications, industrial plants, and so forth.”

Despite the potential benefits, cyber warfare poses challenges to the principle of proportionality. The line between military networks and civilian networks is blurred. As a result, determining how the LOAC applies has proven difficult. Consequently, this uncertainty may lead some countries to launch cyber-attacks against civilian targets in a manner that would be “impermissible under the laws of kinetic war.” Some experts recommend creating a Cyber war National Guard to protect civilian infrastructure. While this approach helps ensure private networks are protected, it leaves unanswered how the U.S. government can launch an offensive cyber-attack.

IV. DOES EXISTING WAR LAW APPLY TO CYBER ATTACKS AND THE NON-STATE ACTORS WHO COMMIT THEM?

Currently, no treaty exists to expressly regulate international cyber-attacks. As a result, a state must rely upon either existing international or domestic law to address them. Domestic laws would be inadequate for a cyber-warfare and its attacks. First, cyber-attacks are “global in nature.” They occur in cyberspace, which involves thousands of interconnected networks across the globe. Second, addressing cyber-attacks under domestic law would leave each individual state to act alone. Moreover, “[i]nternational laws further establish uniformity and clarity where numerous domestic laws may not.” Accordingly, the threat of a cyber-attack within a global cyberspace requires a global solution.

Nevertheless, whether existing international war laws adequately apply to a cyber-attack is a highly debated issue among legal scholars. Because no

154. Id.
155. Id.
156. Kesan, supra note 101, at 431.
157. Id. at 457.
158. Id. (citing Susan W. Brenner with Leo L. Clarke, Civilians in Cyberwarfare: Conscripts, 43 VAND. J. TRANSNAT’L L. 1011, 1064 (2010).
159. Mathew J. Sklerov, Solving The Dilemma of State Responses to Cyberattacks: A Justification For the Use of Active Defenses Against States Who Neglect Their Duty to Prevent, 201 MIL. L. REV. 1, 6 (2009).
160. Id.
161. DeLuca, supra note 30, at 305.
162. Id.
163. Id.; see also Hathaway, supra note 12, at 880.
164. DeLuca, supra note 30, at 305; see also Hathaway, supra note 12, at 822.
165. DeLuca, supra note 30, at 306.
166. Scott J. Shackelford & Richard B. Andres, State Responsibility For Cyber Attacks: Competing Standards For a Growing Problem, 42 GEO. J. INT’L L. 971, 993 (2011); Hathaway, supra note 30, at 844; see also DeLuca, supra note 30, at 296.
specific provision in the U.N. Charter addresses cyber warfare\(^{167}\), the split has focused on whether new international laws should be created to address the ever-evolving nature of cyber-attacks.\(^{168}\) For existing war laws to apply, a cyber-attack must be either a “use of force” under Article 2(4) of the U.N. or an “armed attack” under Article 51.\(^{169}\) Thus, much of the debate has focused on whether a cyber-attack can ever qualify as a “use of force” or an “armed attack.” Second, given the ease with which non-state actors can launch a cyber-attack, another unsettled question hinges on whether a cyber-attack launched by a non-state actor can trigger the LOAC and the victimized state’s right of self-defense under Article 51.\(^{170}\) The first section will analyze whether a cyber-attack constitutes an “armed conflict,” while the second section will discuss whether a non-state actor can create an “armed conflict” and a corresponding right of the victimized state to self-defense.

A. Does a cyber-attack constitute an “Armed Attack?”

Article 51(1) of the U.N. Charter states, in part, that “[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations.”\(^{171}\) To determine whether a cyber-attack constitutes an “armed attack,” a person must interpret the Charter in “good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.”\(^{172}\)

In determining whether any weapon, including a cyber-attack, constitutes an “armed attack,” the type of weapon used is immaterial.\(^{173}\) In an advisory opinion interpreting article 51 of the U.N. Charter, the ICJ stated that it “do[es] not refer to [any] specific weapons. They apply to any use of force, regardless of the weapons employed.”\(^{174}\) Subsequently, the U.N. Security Council reaffirmed this view when it identified a hijacked airplane an “armed attack.”\(^{175}\)

To determine whether a cyber-attack constitutes an “armed conflict,” legal scholars have focused on the following approaches to guide the analysis. The

\(^{167}\) See DeLuca, supra note 157, at 296.
\(^{168}\) See sources cited in supra note 168.
\(^{169}\) Charter art. 2, para. 4; art. 51.
\(^{171}\) Charter art. 51.
\(^{173}\) Gervais, supra note 164, at 542.
\(^{174}\) Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 244 (July 8).
\(^{175}\) Gervais, supra note 164, at 543 (noting that the U.N. Security Council authorized the United States to respond forcefully in self-defense to the 9/11 attacks).
first approach is the instrumentality or instrument-based approach. Under the instrument-based approach, a cyber-attack does not constitute an “armed attack” because it lacks the features of a traditional weapon. Thus, “only traditional weapons with physical characteristics can constitute armed force required to carry out armed attacks.”

To support this approach, scholars point to Article 41 of the U.N. Charter. Article 41 states that complete or partial disruption of “telegraph, radio, and other means of communication” does not involve the use of “armed force.” An “armed force” is a type of “force” under article 2(4). Thus, because the purpose of many cyber-attacks is to disrupt the cyberspace networks designed for communication, a cyber-attack alone is not an “armed conflict” unless “more or different forms of aggression must be shown in order [for the cyber-attack] to constitute an ‘armed attack’ under the U.N. charter.”

A second approach is the target-based approach. The target-based approach focuses less on the weapon used than it does the target of the attack. Under the target-based approach, a cyber attack can constitute an armed attack if it attacks a nation’s critical infrastructure. Critical infrastructure is the “collection of systems that are essential to a state’s well-being, including banking, communications, utilities, emergency services, and transportation.” Roughly eighty percent of the critical infrastructure in the U.S. is owned by private entities.

The third approach is the effects-based or consequence-based approach. Unlike the first two approaches, the effects-based approach does not focus on the weapon used or the target; rather, it focuses on the effects of the cyber-attack. Under the effects-based approach, a cyber-attack can constitute an “armed attack” if the “effect of the cyber-attack is equivalent to that of an armed attack

\[\text{176. Sheng Li, When Does Internet Denial Trigger the Right of Armed Self-Defense?, 38 YALE J. INT’L L. 179, 186 (2013).}\]
\[\text{178. Id.}\]
\[\text{179. Charter art 41.}\]
\[\text{180. Sheng Li, When Does Internet Denial Trigger the Right of Armed Self-Defense?, 38 YALE J. INT’L L. 179, 184 (2013).}\]
\[\text{182. Id.}\]
\[\text{183. Id. at 187.}\]
\[\text{186. Id.}\]
carried out by physical weapons.” Generally, the effects-based approach requires that the damage cause death and destruction to property.

A fourth approach, the sovereign-based approach, holds that a cyber-attack can constitute an “armed attack” if the attack interferes with a state’s right of sovereignty. Under the sovereign-based approach, the focus is not on the instrument or effect, but it is on the “object and character” of the actor’s actions. The sovereign-based approach has received little attention and development since its inception and a more thorough analysis is beyond the scope of this note.

Borrowing from the effects-based approach, a fifth approach is called the non-kinetic effects approach. Under the non-kinetic effects approach, a cyber-attack constitutes an “armed attack” if the non-kinetic effects create consequences that “implicate its victims’ right to survival in a manner equivalent to activities that Charter framers unquestionably considered to be armed attacks.” Upon passage of the U.N. Charter, the Framers understood that at least one, non-kinetic effect constituted an “armed attack”: naval blockades. “Blocking the right of common access to the sea can constitute an armed attack if it seriously disrupts commerce and communications so as to threaten victims with strangulation or economic ruin.” Thus, the Framers understood that serious disruptions in commerce and communication from blocking naval blockades can constitute an “armed attack.” It follows that by classifying the internet as a common property similar to a naval blockade, cyber-attacks that cause serious enough disruptions in commerce and communication can constitute an “armed attack.”

B. Can a victim state assert self-defense against a territorial state for a cyber-attack caused by a non-state actor within the territorial state?

Traditionally, the principal actors of war and conflict on the world stage were nation-states. Nation-states, or states, have a legally-recognized status among the international community. Non-state actors, on the other hand, lack such legal status. Nevertheless, since World War II, the world has experienced a

188. Id.
190. Id.
191. Li, supra note 181, at 191.
192. Id.
193. Id.
196. DeLuca, supra note 188, at 291.
significant increase in non-state actors becoming actors in world politics and war. For example, on September 11, 2001, the U.S. suffered one of the worst terrorist attacks in its history. These deadly attacks were launched by a terrorist organization, not an official state. Today, the cyber warfare from non-state actors currently dominates the cyber battlefield. “With an increasing number of cyber-attacks originating from sophisticated cyber criminals, “hackivists,” and State-sponsored patriotic hackers, a new era of cyber-warfare is emerging.”

Accordingly, one of the greatest challenges regarding the rise of cyber warfare is the potential for these attacks to come from non-state actors. As cyberspace grows in popularity, so too will the recruitment of more non-state actors to engage in cyber-attacks. For example, during the cyber-attacks against Georgia, “[w]ebsites displayed how-to guides providing eager individuals step-by-step instructions on how to configure their computers to attack Georgian websites.” Moreover, “[o]ther websites coordinated the volunteers by posting the statuses of target sites.” This kind of recruitment to galvanize cyber-attacks heightens the concern that non-state actors will play a larger role in cyber-attacks moving forward.

Despite the grave havoc that non-state actors can wreak in world politics and conflict, whether a non-state actor can commit an “armed attack” under article 51 of the U.N. Charter has been the subject of scholarly debate. The eventual determination of this debate is significant. If a non-state actor cannot commit an “armed attack,” then the LOAC does not apply, and the victim state that was attacked cannot invoke its right of self-defense. Thus, non-state actors could launch cyber-attacks from anywhere with an internet connection from another state, knowing that the target cannot respond to it. However, if a non-state actor can commit an “armed attack,” the victim state has a set of tools available to ensure that it can protect its security.

One group holds that “armed attacks” can be committed only by state actors. This view finds support in the language of the U.N. Charter. Under article 2(4), only a state can engage the “use of force.” Following the logic that an “armed attack” is a more narrow form of “force,” then a state can only

197. Id.
200. Id.
201. DeLuca, supra note 188, at 279.
203. Id.
205. Id.
commit an “armed attack.” Moreover, in a 2004 Advisory Opinion, the ICJ concluded that Article 51 recognized only “the existence of an inherent right of self-defense in the case of armed attacks by one state against another state.”207

A second group rejects the ICJ’s advisory opinion and holds that a non-state actor can commit an “armed attack,” but only if the attack was attributable to a state.208 First, although Article 2(4) prohibits the “use of force” by a state, article 51 is silent as to the specific type of actor that can commit an “armed attack.”209 Moreover, even in the 2004 advisory opinion, the majority recognized that a non-state actor’s actions may be “imputable” to a state actor.210 The use of “imputable” parallels the principle of attribution, asks whether an attack can be attributed to a state.211

To determine whether a victim state can attribute a cyber-attack to a specific state, international courts use two competing standards: effective control and overall control.212 Under effective control standard, the non-state actor must act in “total dependence” upon the state actor, while the “overall standard” attributes state responsibility when it is involved in “equipping, financing, training, along with limited supervision.”213 Thus, the overall control holds a state responsibility for acts of a non-state actor if it offers “instruction and guidance, though it need not have had complete control.”214

Although the effective control and overall control standards have prevailed in the legal community, a third standard could gain traction: blind-eye control. The blind-eye standard emerges from existing interpretations by the ICJ. The problem would arise when a state argues that, although it knew a non-state actor intended to and eventually did launch an attack, it did not exercise any control over that process. Here, the ICJ imposes upon every state a duty to “not to allow knowingly its territory to be used for acts contrary to the rights of other states.”215 Following this logic, “a state may not knowingly allow non-state actors within its borders to attack another state.”216 Specific to cyber-attacks, international law already requires states to take reasonable precautionary steps to prevent cyber-attacks.217 For example, the Convention on Cybercrime “requires signatories to

208. Deeks, supra note 198, at 492.
209. Charter art 51
210. Wall I.C.J. 136
211. Wall, I.C.J. 136
213. *Id.* at 203-04.
214. *Id.* at 204.
217. *Id.*
adopt domestic laws that criminalize cyber-attacks.” Thus, the blind-eye control standard holds that:

If a state knowingly allows--either through action or omission--a non-state actor to commit an attack, the state would be held internationally responsible. But if the state undertakes sufficient measures to protect other states, and a cyber-attack still manages to originate from its territory, the state would not be responsible.

In practice, however, the blind-eye approach will likely lead many states to claim ignorance or refuse to exercise the degree of care necessary to discover whether a non-state actor intends to execute a cyber-attack from within its territory.

Finally, the third group recognizes that a non-state actor can commit an “armed attack, “regardless of whether a state was involved in any aspect of the attack.” The third group parallels the second group, but it picks up where the blind-eye control standard has left off. This approach is premised on the theory that a non-actor can commit an “armed attack” even if the state in which the non-state actor is located has no knowledge of the attack. This approach is not without merit. First, as noted, Article 51’s text is silent on the specific actor that can commit an “armed attack.” To that end, three judges dissented in the same 2004 advisory opinion, including Judge Buergenthal, who recognized that a non-state actor could commit an “armed attack” without depending on a state actor.

Within the third group, two competing sub-groups exist. The first sub-group, unwilling or unable sub-group, presupposes that the cyberspace within a state’s territory is owned by the particular state, while the second sub-group, common property sub-group, advocates that cyberspace is common property enjoyed equally by all states. Ostensibly, both sub-groups developed their theories based on the principle of neutrality.

Under the principle of neutrality, during a conflict, a belligerent- actor launching a cyber-attack- cannot move weapons across a neutral site. The proponents of the unwilling and unable sub-group argue that

---

218. Id.
219. Id. at 549.
221. Id.
222. Charter art 51.
223. Wall I.C.J. 136, P 6 (separate declaration of Judge Buergenthal).
226. Id.
a cyber-attacker uses the cyberspace of the territorial state to move the weapon-
the attack across its territory.

In applying the theory to the sub-group, the unwilling and unable sub-group argues that after a non-state actor has launched a cyber-attack, the territorial state-the state in which the non-state actor is located-has a duty to suppress the cyber-attack and prevent further attacks.227 Here, a victim state may invoke its right of self-defense against a territorial state for an armed attack caused by a non-state actor within the territorial state, if the territorial state is “unable or unwilling” to suppress the threat.228 To invoke the unable or unwilling doctrine, the victim state must assess whether the territorial state is able or willing to suppress the threat caused by the non-state actor.229 If the territorial state is able or willing, the victim state cannot invoke self-defense against it within the territorial state, but if the territorial state is not able or willing, then the victim state can invoke its right of self-defense.230 Proponents of this sub-group argue that the U.S. has implicitly endorsed this view. For example, in May 2011, U.S. military personnel entered Pakistan without pre-approval from Pakistani officials to capture or kill Osama bin Laden.231 Pakistan’s government objected to the unilateral action, but the U.S. kept Pakistan in the dark because it was concerned that such knowledge may compromise the mission.232

Some legal scholars argue that the unable or unwilling analysis is meritless when handling a cyber-attack because of the exception within the principle of neutrality.233 The exception states that a neutral is not prohibited from restricting “the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals.”234 However, the proponents of this sub-group argue that “nothing in 1907 Hague Convention V suggests that this exception applies beyond communications infrastructure to digital systems that actually generate information, such as satellite imagery, weather, and navigation systems.”235

The common property sub-group has proposed a novel concept to understanding cyber warfare. Common property includes outer-space and the high seas.236 This sub-group would not hold a state responsible for the cyber-

---

227. Deeks, supra note 218, at 493.
228. Id. at 487.
229. Id.
230. See id.
231. Id. at 485.
234. Id.
attacks of a non-state actor within its territory. However, it fits into this sub-group because the victim state would be allowed to assert a right of self-defense against the non-actor state using the same cyberspace networks that the cyber-attacker used, including a territorial state’s cyberspace. Under this theory, although a territorial state would be immune from any duties to stop, prevent, or suppress a cyber-attack, the victim state would allowed to use the common property of cyberspace to respond to a cyber-attack.

Critics have identified two problems. First, existing common properties are not created by humans, they are discovered by them. Thus, because no person created any global commons, no entity has rights to them. Applying the concept here, cyberspace and the internet were created, and accordingly, they cannot be a global common property. Second, even common properties are not entirely free from territorial jurisdiction. For example, the high seas become common property only “beyond 200 nautical miles and outer space above an altitude of approximately 100 kilometers.” But the proponents respond that this strengthens the argument that cyberspace can be a hybrid between a common property and territorial. For example, in the polar archipelago of Svalbard, the ecological resources are considered for the common benefit of multiple nations, but Norway bears the “legal responsibility and cost of administering most of the island’s territory.”

Applying the logic to cyberspace, a hybrid approach may require a state to exercise control over cyberspace to prevent and suppress cyber-attacks while allowing the other activity to be open to all. However, cyberspace is not separate from the physical servers and computers that connect to it. The servers and computers are located within a specific territory, but it does not follow that cyberspace must be specific to a region.

V. ANALYSIS AND PROPOSAL: A VICTIM STATE CAN ASSERT ITS RIGHT OF SELF-DEFENSE AGAINST A CYBER-ATTACK BY A NON-STATE ACTOR

Although critical treaties that govern the conduct of war were last modified in the wake of World War II, the U.N. Charter’s text, history, and ability to adapt to modern times confirms that a cyber-attack can constitute an “armed attack” under article 51 of the U.N. Charter. To determine whether a cyber-attack constitutes an “armed attack,” the non-kinetic effects-based approach

---

237. Id.
238. Id.
239. Id. at 1576.
240. Id.
242. Id. at 1579-80.
should govern. Also, a victim state can assert a right of self-defense against a territorial state for cyber-attacks launched within that state’s territory. In asserting the right of self-defense, this Note proposes that the victim state should comply with the principles of the LOAC as it relates to both civilian and military objects to the territorial state when defending itself from a cyber-attack.

A. Cyber-Attack Can Constitute An Armed Attack

1. The war laws are adaptable

Some legal scholars argue that the LOAC applies only to physical weapons, and thus, is outdated and unable to adapt to modern cyber warfare. However, the issue of whether a new weapon of war is governed by existing international law is not new. With each advancement in technology producing a new, modern weapon, world leaders and legal scholars have debated and disputed whether new international war laws were necessary. During the Civil War, Union allies sent a letter to its General-in-Chief stating that “ever since the beginning of our present War, it has appeared clearer and clearer to me, that the President ought to issue a set of rules and definitions providing for the most urgent cases . . . on which our Articles of War are silent.”

Further, during the Cold War, some argued that the weapons of that era had “inconveniently by-passed [the] Queensberry-like practices” under the U.N. Charter. With each passing generation, world leaders have argued that international war law was inadequate to address the modern weapons of the time. However, despite the critics, the LOAC has adapted. For example, at the time of passage of the Charter, the Framers did not contemplate a battle in space. Yet, the U.S. has unequivocally held that “[p]urposeful interference with U.S. space systems will be viewed as an infringement on [the] sovereign rights [of the United States]. The U.S. may take all appropriate self-defense measures . . . to respond to such an infringement.” Cyber warfare is no different, and the existing laws should apply to it.

245. See id.
248. Memorandum from William Cohen, Sec’y of Def. for Sec’y of the Military Dep’ts et al., Department of Defense Space Policy, at 3 (July 9, 1999)).
2. The right approach for a cyber-attack to constitute an “armed attack”

Even assuming an adaptable LOAC, other scholars argue that the existing instrument-based, target-based, and effects-based approaches are inadequate.\(^\text{249}\) To be fair, the instrument-based and target-based approaches have serious flaws. Recall, the target-based approach holds that only physical weapons can constitute an “armed-attack” based on the language found in article 41 of the U.N. Charter.\(^\text{250}\) The target-based approach is flawed for two reasons. First, it is “unable to meet modern national security challenges.”\(^\text{251}\) Additionally, “[t]here are textual counter-arguments, such as that Article 51’s more specific limit to “armed attacks” suggests that drafters envisioned prohibited “force” as a broader category not limited to particular methods.”\(^\text{252}\) Finally, even the ICJ has concluded that an “armed-attack can occur, regardless of the weapon used.”\(^\text{253}\)

The targets-based approach can be over inclusive. If, for example, any cyber-attack that targeted critical infrastructure constituted an “armed conflict,” then many states may construe espionage efforts as triggering their right of self-defense. Even assuming this approach is not over inclusive, the fragmentation of the current international understanding regarding cyber-attacks gives this approach pause. To understand the danger of such fragmentation, Harvard law professor Jack Goldsmith has explained, “[o]ne nation might do something that another nation takes to be an act of war, even when the first nation did not intend it to be an act of war.”\(^\text{254}\)

The effects-based approach is not without benefits. The effects-based approach is the most attractive among legal scholars and it has been endorsed by the Departments of State and Defense.\(^\text{255}\) This approach “adopts an evolving definition that permits non-physical force—such as electronic jamming, directed-energy weapons, and cyber-attacks—to fall under the umbrella of military force.”\(^\text{256}\) However, it is limited. Many of the proponents of this approach hold that “only cyber-attacks that proximately cause kinetic effect or physical damage

\(^{249}\) Christopher D. DeLuca, *The Need for International Laws of War to Include Cyber Attacks Involving State And Non-State Actors*, 3 No. 9 PACE INT’L L. REV. ONLINE COMPANION 278, 296 (2013).


\(^{253}\) Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 244 (July 8).


\(^{255}\) Hollis, supra note 244, at 1041.

can qualify as armed attacks.” 257 Thus, a cyber-attack can constitute an “armed attack” only if it causes kinetic-effects: death or destruction of property. But such a restrictive view “leaves unregulated the very aspects of [cyber-attacks] that make it so novel.” 258

This is a flawed theory. In essence, this rigid line of thinking “treat[s] combat-enabling cyber-attacks that do not produce kinetic effects, such as disabling enemy air defenses with a virus, differently from attacks that knock out those systems with missiles over bombs, even though both methods yield identical battlefield results.” 259 Under a purely effects-based approach, even the same effect can be treated differently based on the manner the attacker used. Such a legal theory would produce bizarre results. Additionally, a purely effects-based approach fails to consider that a cyber-attack that wipes “out financial records or disrupting telecommunication networks can have catastrophic effects on civil society.” 260 For example, the cyber-attacks on Estonia cost it a total equivalent to roughly 5% of its overall economic activity, 261 but under the effects-based approach, it would have been powerless to respond.

The non-kinetic effects-based approach is the most effective in finding that a cyber-attack can constitute an “armed attack” under the Charter, and the most consistent with the intent of the Framers of the Charter. Additionally, it satisfies the chief concerns among the critics of the effects-based approach, who claim that such approach fails to consider effects that do not cause death or destruction to property. 262

The non-kinetic effects-based approach reflects the Framers’ intent. Article 42 lists certain actions that are prohibited and constitute illegal force, unless the U.N. Security Council has authorized otherwise. 263 The list includes blockades. 264 Accordingly, at the time the Charter was enacted, the Framers understood a blockade to be inconsistent with the Charter, unless the U.N. Security Council authorized it. However, a blockade does not necessarily involve kinetic force. 265 A blockade is a denial to another entity to access a port. To conduct a blockade, a state may deny another state maritime access or a ship

257. Id. at 188.
258. Hollis, supra note 244, at 1042.
261. Id. at 201.
263. Charter art 42.
the ability to communicate with a port.\textsuperscript{266} Initially, the international community did not recognize a blockade as an act of war, unless one party engaged in kinetic force, or physical death or destruction.\textsuperscript{267} However, by the mid-Twentieth Century, the controlling thought recognized a blockade, alone, as an act of war.\textsuperscript{268} For example, in 1956, Egypt blocked Israel’s access to the Strait of Tiran, and as a result, Israel requested to the U.N. its right of self-defense under Article 51.\textsuperscript{269} The international community accepted this position.\textsuperscript{270}

The destruction from the blockades are not kinetic, but they strangulate economic ruin, and “they disrupt commerce and communications, and their indirect effects on social welfare are often the intended aim for which they were employed.”\textsuperscript{271}

To be fair, although a blockade does not, itself, involve kinetic force, the enforcement of a blockade might involve a kinetic response. Thus, some may argue that the purpose of the blockade listing in Article 42 is to discourage the threat of violence. But the same logic can apply to cyber warfare in the modern world. As the world becomes increasingly dependent upon cyberspace, denying or disrupting access to it will threaten substantial economic activity and emergency responses, magnifying the risk of a violent response.

3. The U.S. rightfully has recognized the effects-based approach

In recent history, the U.S. has implicitly endorsed the non-kinetics effects-based approach. In defending its right of self-defense against an attack on its space technology, the U.S. concluded that “[t]he ability to access and utilize space is . . . critical to U.S. national security and economic well-being.”\textsuperscript{272} The DOD has stated that intentional interference with U.S. Space Systems would necessarily interfere with the sovereignty of the U.S.\textsuperscript{273} In outlining this boundary, the U.S.’s analysis was silent about whether the space attack must be kinetic. Moreover, the National Research Council Committee, entrusted to research cyber issues, has also favorably reacted to this approach.\textsuperscript{274} In 2010, then Secretary of State Hillary Clinton outlined that the U.S. intended to defend

\textsuperscript{266} Id.
\textsuperscript{267} Id.
\textsuperscript{268} Id.
\textsuperscript{271} Id. at 195.
\textsuperscript{272} Memorandum from William Cohen, Sec’y of Def. for Sec’y of the Military Dep’ts et al., Department of Defense Space Policy, at 2 (July 9, 1999).
\textsuperscript{273} Id.
\textsuperscript{274} OFFENSIVE INFO. WARFARE, NAT’L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK Capabilities 33-34 (2009).
“its cyber-security in terms similar to those usually used to discuss military security and self-defense.”

A non-kinetic effects-based approach serves the U.S.’s national interest. Historically, the U.S. favored a restrictive interpretation of “armed attack” under the Charter. A restrictive interpretation protected the U.S. from physical attacks while allowing it, the wealthiest nation in the world, to impose tough economic sanctions. However, cyberspace and the Twenty-first Century have reshaped modern warfare and the likely players involved. Now, because of the widespread use of the internet and low-cost of launching a cyber-attack, the U.S. has become vulnerable to a widely damaging cyber-attack from any country or terrorist organization with an internet connection. This allows developing states with inadequate military resources to use its cyber resources to create a more level playing field in the modern-era of war.

To combat this momentum, the U.S. should favor a more expansive interpretation of the Charter with respect to cyber warfare. The benefits are twofold. First, an expansive interpretation would allow the U.S. to assert the right of self-defense against a cyber-attack. This is critically important because roughly eighty percent of “internet traverses through the United States, chiefly through servers owned by private enterprises.” Second, the non-kinetic effects-based approach would exclude certain types of cyber activity that the U.S. may not want within the purview of international war law. For example, “[c]omputer-based espionage, intelligence collection, or even some preemptive cyber-operations or countermeasures designed to disable an adversary’s threatening capabilities” would not create the effects necessary to reach the threshold of “force” or “armed attack.” The result would be that the U.S. could continue engaging in information-gathering and other beneficial national security measures without violating international war law. Perhaps the U.S.’s hesitancy in creating a line-drawing standard on cyber warfare is a consequence of its attempt to balance its vulnerabilities to cyber attacks and its advantages to information-gathering measures.

4. Cyberspace: a hybrid form of common property
   a. Cyberspace as common property

---

276. See id. at n.25.
277. See id at 449.
279. Waxman, supra note 269, at 443.
280. Id. at 434-35.
To endorse the non-kinetic effects-based approach, this note proposes that cyberspace be recognized as a hybrid form of common property: common property for purposes of availability and territorial for purposes of responsibility. This approach reflects the Framers’ intent, resolves the problem with a purely effects-based approach, and preserves each state’s responsibility to prevent cyber-attacks.

Under customary international law, the right of maritime common access is enjoyed by all nations. As noted in Section IV, Part A, the Framers of the U.N. Charter understood that blocking maritime access could constitute an “armed attack.” The premise of this right stems from the reality that the world offers common property that all nations should share without interruption.

As technology developed, however, the right of common property evolved to include “international airspace and outer space, it also came to govern telecommunications media.” Today, the U.N. recognizes internet access to be essential for human rights. Therefore, blocking access to the internet and cyberspace should be construed similarly to blocking access to ports, airspace, or outer space. This approach resolves the concern that the kinetics effect-based approach is misguided, because it fails to recognize the potential effects of a cyber-attack that may not reach physical destruction but nevertheless cause substantial damage.

b. The Critics of cyberspace as a common property

The novel idea of defining cyberspace as common property is not without critics. First, they argue that global commons have all been pre-existing regions through discovery. Thus, because no person created or developed any global commons, no entity has rights to them. This criticism is not without merit. At first glance, the internet was not discovered, but it was created by a military program decades ago. But this is not dispositive and can be overcome. The

282. Charter art 42.
284. Id. at 192.
285. Id.
288. Stevens, supra note 280, at 659.
international community has come to recognize the common right of access to telecommunications, telegraphs, and radio, all of which were human created.\textsuperscript{289}

Second, even pre-existing global commons are not entirely free from territorial jurisdiction.\textsuperscript{290} Indeed, states have tried to exercise control over the internet within their territory.\textsuperscript{291} To justify such control, legal scholars argue that like other tangible objects, cyberspace is comprised of tangible objects, and accordingly, states can exert jurisdiction over it.\textsuperscript{292} For example, states have regulated internet routers and the internet’s content.\textsuperscript{293} Moreover, the critics argue that a common property approach would be harmful to innovation because “[h]istory has shown that such systems lack adequate investment and innovation since no single entity can reap the full benefit of its own contributions.”\textsuperscript{294}

But this criticism dovetails conveniently into existing common property. Existing common property does not enjoy an absolute right of access. For example, the high seas become common property only “beyond 200 nautical miles and outer space above an altitude of approximately 100 kilometers.”\textsuperscript{295} Thus, even existing common property, including the high seas, shares both a common element and a jurisdictional element, giving credence to a hybrid approach for cyberspace.

This is not to suggest that the internet and the sea are entirely identical. The sea, for example, has shorelines separate from the oceans. The internet, however, is comprised of servers, nodes, and computers, all of which have physical locations. Therefore, the notion that cyberspace cannot be separated from its physical features is not without merit. Moreover, cyber attackers target the physical computers, networks, and servers when launching a cyber-attack. Unquestionably, this dynamic poses challenges. However, given the ability of states to control parts of cyberspace, including blocking certain websites, it should not be impossible to overcome.\textsuperscript{296}

5. The proposal: a hybrid approach

The international community should consider cyberspace a hybrid between a common property right of access for all and a jurisdictional duty of care to all.

\begin{itemize}
\item \textsuperscript{289} Francis Lyall, International Communications: The International Telecommunications Union and the Universal Postal Union 50, 55-70 (2011).
\item \textsuperscript{290} Sean Kanuck, Sovereign Discourse on Cyber Conflict Under International Law, 88 TEX. L. REV. 1571, 1576 (2010).
\item \textsuperscript{291} Id.
\item \textsuperscript{292} Id.
\item \textsuperscript{293} Id.
\item \textsuperscript{294} Id. at 1576
\item \textsuperscript{295} Id.
\item \textsuperscript{296} For example, a car bomber inevitably travels down a public road in order to reach his or her target location. Assuming the target building is not government owned the territorial government cannot control or provide security at the private building, but it can control the means by which the car bomber travels: the public road system.
\end{itemize}
To do so, a decision regarding which parts should be collectively governed and which should be given state control should be evaluated. This note contends that, as a beginning point, access should be granted to all, and each state should have a duty to prevent and suppress a cyber-attack launched from within its territory.

This approach already exists today. For example, in the polar archipelago of Svalbard, the ecological resources are considered for the common benefit of multiple nations, but Norway bears the “legal responsibility and cost of administering most of the island’s territory.” 297 Another example is the international waterways. The waterways such as inland rivers, straits, and lakes with common right of access are within the control of adjacent countries, but such control is not absolute. 298

Additionally, the DOD approaches cyberspace as a uniquely man-made domain, unlike air, space, and water domains. 299 In explaining the DOD’s position, Major Erik M. Mudrinich has given credence to the notion that the internet is a global common. 300 For example, Major Mudrinich has stated: “[a] modern society and military cannot effectively operate without cyberspace. If cyber capabilities are denied, we could descend quickly from a digital-age to a dark-age in a matter of moments.” 301

Accordingly, a cyber attack that causes physical destruction or death constitutes an armed attack. Even if a cyber-attack does not cause physical destruction or death “but is of sufficient scale and effect to threaten the target state with strangulation or economic ruin, it constitutes an armed attack.” 302 This incorporates the non-kinetic effects-based approach. To determine whether such a non-kinetic cyber-attack rises to the level of an armed attack, the same analysis used for kinetic damage should apply. The analysis would include the level of vulnerability of the victim state and impact on its digital infrastructure. Thus, the more dependent a state on cyberspace, the more vulnerable it is, and accordingly, the smaller the cyber-attack would be needed to trigger an armed attack.

**B. A Victim State Can Assert Self-Defense Against A Territorial State For a Cyber-Attack Launched by a Non-State Actor**

Under international law, states have a “duty to prevent non-state actors within their borders from committing cross-border attacks.” 303 Accordingly, a

---

297. Kanuck, supra note 284, at 1579.
300. Id.
301. Id.
303. Mathew J. Sklerov, Solving The Dilemma of State Responses to Cyberattacks: A Justification For the Use of Active Defenses Against States Who Neglect Their Duty to Prevent, 201
state has a duty to prevent a non-state actor from launching a cyber-attack from within its borders.\textsuperscript{304} In doing so, the doctrine of proportionality would permit a victim state to respond to a non-state actor attack by invoking self-defense not only against the non-state actor, but also the state from where the attack occurred.\textsuperscript{305} Regardless of whether the international community adopts the “unable or unwilling” approach, common property approach, or the telecommunications exception to neutrality, the victim state can assert this right of self-defense.

The effective control and overall control are good starting points, but they require a certain level of state involvement in the cyber-attacks. In the modern world of war, many non-state actors launch attacks without approval or knowledge from the territorial state in which the non-state actor resides.

1. Unwilling or Unable: The Way Forward

The unwilling or unable approach offers the best way forward. Also, it is not difficult to understand under existing war law. First, the ICJ has given credence to the idea that a state actor can be responsible for attacks “imputed” to it.\textsuperscript{306} Second, on land, a neutral has a duty to prevent a belligerent from using its terrain to move or mobilize war materials and supplies across the land.\textsuperscript{307} Also, a neutral cannot supply “troops, war material, or the means of producing war material.”\textsuperscript{308}

To be fair, the unable or unwilling approach presupposes that the cyberspace within a state is owned by that state. This is consistent with this Note’s contention that cyberspace should be a hybrid common property. For purposes of common property, an understanding of a neutral’s duty with respect to high seas is important. Indeed, under international law, states must use the seas for peaceful purposes and refrain from engaging in “force” under article 2(4) of the U.N. Charter, subject to the right of self-defense under article 51.\textsuperscript{309} Additionally, however, a belligerent cannot use neutral ports and waters or territory waters as a place for naval operations.\textsuperscript{310} To enforce this rule, the neutral state has a duty to use the resources at its disposal. If a neutral is


\textsuperscript{306} Wall, I.C.J. 136


\textsuperscript{308} Id.

\textsuperscript{309} Id. at 1151.

\textsuperscript{310} Id. at 1157.
unwilling or unable to “enforce its duty to clear waters of belligerent forces,” a victim state may act against the belligerent forces present in neutral waters.\textsuperscript{311}

Applying these principles here, a cyber-attack is a form of modern-day weapon. In addition to analysis above, the U.S. has recognized the powerful potential of a cyber-attack as a weapon. The White House Cyberspace strategy states:

When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense ... We reserve the right to use all necessary means--diplomatic, informational, military and economic-as appropriate and consistent with applicable international law in order to defend our nation, our allies, our partners, and our interests.\textsuperscript{312}

Moreover, if the territorial state is unwilling or unable to suppress the threat of a cyber-attack across its cyberspace networks, the victim state can assert its right of self-defense. Nevertheless, the victim state must respect the territorial state’s sovereignty to the extent it can without sacrificing its own security. To strike the right balance, a victim state should be able to respond to a non-state actor within a territorial state if it exercises the principles of distinction, proportionality, and humanity against both civilian and military objects of the territorial state. Thus, the victim state would honor the LOAC as it applies to objects within the territorial state and only respond in self-defense to the extent consistent with these principles to counter the cyber-attack.

2. Effect on the principle of attribution

This approach will help resolve the problem with the principle of attribution. Absent attribution, a “victim state cannot lawfully launch a response without knowing the identity of the attacker.”\textsuperscript{313} Additionally, without attribution, “those who would attack us suffer little fear of reprisal and will continue to declare open season on the testing, breaching and compromise of U.S. networks.”\textsuperscript{314} Indeed, the U.S. will need to properly attribute a cyber-attack to the right territorial state, even if the attack is launched by a non-state actor.

As noted, attribution can be difficult. Some U.S. officials claim that attribution is the single, greatest challenge to cyber warfare.\textsuperscript{315} The cyber-attacks are “taking advantage of the fact that routing an attack through countries that are

\textsuperscript{311}. Id.
\textsuperscript{314}. Id. at 188.
\textsuperscript{315}. Id. at 195.
not on the best of terms with the target country will effectively conceal their identity and location.\footnote{The Technolytics Institute Cyber Warfare Center, Cyber Commander’s eHandbook: The Weaponry and Strategies of Digital Conflict, 10-13 (Jan. 2010), available at http://www.technolytics.com/CyberWarfare.asp.}

However, if this happens, the victim state is not powerless. Charged with the duty to prevent and stop cyber attacks within its territory, the territorial state should be imputed with responsibility for a cyber attack launched within its territory to the extent that the victim state can respond consistent with the LOAC. Also, the victim state can put the territorial state on notice of such use of its cyberspace to launch an attack, and if the territorial state is unable or unwilling to suppress the threat, the victim state can counterstrike using the same networks, despite their original status as neutral. This counterstrike is not unlimited. The victim state must comply with the LOAC. And although the principle of distinction requires separation from civilian and non-civilian objects, the principle of proportionality creates an exception to it. Thus, the victim state can interfere with innocent objects if it respects the principle of proportionality.

Indeed, this is a unique approach. However, cyberspace is uniquely qualified to receive a different approach. Cyberspace is unlike any other domain in the history of war. Unlike land, sea, and water, cyberspace has no boundaries and no limits. It connects Wall Street in New York to Main Street in Afghanistan; it empowers a poor terrorist in Iraq to destroy critical infrastructure in Los Angeles. Without this approach, cyber attackers can hide behind a veil while the territorial states can claim their inability to stop or prevent the attacks. At a time when world peace is as important as it has ever been, the U.S. should adopt a policy that holds territorial states as accountable as they have ever been.

3. Telecommunications exception

Some legal scholars argue that the telecommunications exception for a neutral state applies to cyberspace.\footnote{Jeffrey T.G. Kelsey, Hacking Into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare, 106 MICH. L. REV. 1427, 1442 (2008).} As noted, under the exception, a state is not prohibited from restricting “the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals.”\footnote{Id. at 1143.} Thus, if it applied, a state would not have a duty to prevent or suppress any cyber-attack.

Although cyberspace is more than a way to communicate and the exception does not apply, this would not change this Note’s proposal. Under Article III of the 1907 Hague Convention, a neutral state is not “called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus,” so long as the neutral state impartially permits the
use of those structures by all belligerents." But if a non-state actor launches a cyber-attack, the victim state asserting self-defense is also a belligerent. So, even if legal scholars claim that the internet should meet the exception under the law of neutrality, the territorial state should allow the victim state to use the same cyber networks to respond in self-defense to the non-state actor that launched a cyber-attack using the cyber networks.

VI. CONCLUSION

With their low cost and instantaneous nature, cyber-attacks will be a powerful weapon in the wars of the Twenty-First Century. As American life increasingly grows more interconnected and dependent upon cyberspace, the threat and potential effects of a cyber-attack grow fiercer. To prepare for this new reality, existing laws of war should apply to a cyber-attack launched by both state and non-state actors. A victim state should be able to assert its right of self-defense against a territory state for a cyber-attack launched by a non-state actor within the territory state if such state is unable or unwilling to suppress the threat. Even if the U.S. holds that cyberspace meets the telecommunication exception to the principle of neutrality, the victim state should still be able to assert its right of self-defense.

Technology has always revolutionized the landscape of war. During the eighteenth century, the castles and knights gave way to guns, and the twentieth century’s invention of aircrafts threatened to destroy the world by “strategic bombing campaigns during the First World War.” Now, at the break of the twentieth first century, information technology will do the same.


322. Id.