ARTICLES

Mitigating Moral Hazard in Cyber-Risk Insurance
By Liam M.D. Bailey

The Deregulation and Swarming of Cyberwarfare:
The Need for and Limitations of Law in Enabling Aggressive
‘Hacking-back’ and Pre-Emption
By Dr. Mils Hills

Legal Considerations on Cyber-Weapons and Their Definition
By Stefano Mele

Internet Communication Blackout: Attack Under Non-International
Armed Conflict?
By Cassondra Mix

Bitcoin Laundromats for Dirty Money: The Bank Secrecy Act’s (BSA)
Inadequacies in Regulating and Enforcing Money Laundering Laws over
Virtual Currencies and the Internet
By Sheng Zhou
EDITORIAL BOARD

EXECUTIVE EDITORS
Editor-in-Chief
Daniel B. Garrie, Esq.

Executive Editor
Siddartha Rao, Esq.

Research Editor
Radhika Tiwari

INDUSTRY ADVISORS
Alan Roper                     Jonathan Turner
Cedric Leighton                Joseph V. DeMarco
Christopher Burgess           Joseph Weiss
Dick Crowell                   Larry Ponemon
Eric Jensen                   Michael Schmitt
Gus Dimitrellos               Noah Bledstein
Jack Dever                    Richard Borden
James Christiansen           Russell Walker
Jeff Bardin                  Uma Chandrashekhar
Jeremy Kroll                  Vincent Scott
John Dever                    William Spernow

MEMBERS
Kim Kopoff
Candice Lang
Sarah E. Haines
Stephen Williams
Valerie Strumwasser
Margaret Mak
Salvatore Scibetta
Mitigating Moral Hazard in Cyber-Risk Insurance

By Liam M. D. Bailey

Abstract:

Over the last decade, electronically stored data has become both an indispensable asset and emergent liability for companies that transact business online. Almost weekly, data breaches and computer crimes make national headlines, compounding the public’s demand for adequate protection of sensitive consumer information. Increasingly, entities doing business in the information age find that traditional commercial general liability insurance policies do not cover the loss or theft of electronic data, leaving those entities with a sizable gap in insurance coverage in the event of a data breach.

In response to this coverage gap, insurers have begun underwriting cyber-risk insurance policies to specifically address the perils of e-commerce. These policies range from coverage for losses and fines associated with data breach notification statutes, to comprehensive indemnity from consumer class action suits, infrastructure remediation costs and credit monitoring for affected individuals. Similar to more established types of insurance, however, cyber-risk coverage is not immune from the traditional vulnerabilities of the insurance marketplace, including moral hazard and adverse

1 Liam Michael Driscoll Bailey is a third year law student at the University of Connecticut School of Law in Hartford, CT. Liam holds a B.A. in Classics from Gettysburg College and is a native of West Hartford, CT.
This Article seeks to provide insurers and policymakers with a suggestion for mitigating moral hazard in the cyber-risk insurance market. Through an analysis of information security regulation and public policy considerations, this Article proposes an information exchange that insurers and regulators may use to share loss data, claim costs, and compliance audits of insureds, in an effort to more effectively price cyber-risk coverage and thereby reduce the moral hazard presented by insureds that possess insufficient information security infrastructure. Admission to this information exchange is predicated on two conditions: First, an insurer must pledge to discount premiums for entities that employ information security infrastructure that sufficiently protects consumer custodial data as matter of public policy; and second, insurers writing cyber-risk coverage must contribute their own loss data to this information exchange.

The result of this proposal is a recommendation for an information-sharing platform, which encourages insurers to pool loss data and differentiate premiums for preferred risks. Because cyber-risk insurance is neither a market-driven private enterprise engaged in the unrestrained pursuit of profit, nor a tightly regulated, monopolistic public utility, this Article seeks to balance the autonomy of insurers with the public’s need for adequately secured personal information to create a system that simultaneously mitigates moral hazard for insurers while encouraging the adequate protection of consumer data.2

---

2 The author acknowledges and thanks Dr. David Thaw of the University of Connecticut School of Law, without whom this Article could not have been written, D. P. Stock, and the University of Connecticut Insurance Law Center.
I. INTRODUCTION

In April of 2011, Sony Corporation suffered one of the most prominent data breaches of the new millennium. Upwards of seventy-seven million users on the PlayStation® Network, a worldwide online service, were affected when unknown third parties accessed the PlayStation Network without authorization and absconded with the names, addresses, birth dates, passwords, and credit card information of Sony’s subscribers. What made this particular data breach so remarkable, however, was neither the breadth of users affected nor the monetary value of the information that was stolen. Instead, what made the PlayStation Network breach so significant was the response of Sony’s insurer, the Zurich American Insurance Company (“Zurich”).

In July of 2011, Zurich filed an action for declaratory judgment in the Supreme Court of the State of New York, seeking “declaratory relief to settle important questions concerning Sony Defendants’ claims for insurance coverage relating to numerous class action lawsuits, miscellaneous claims, and potential actions . . . arising out of one or more of the cyber-attacks perpetrated by computer ‘hackers’ on the PlayStation Network.”3 Zurich filed this action seeking an affirmative ruling that the insurer was not obligated to indemnify Sony under their commercial general liability or excess umbrella insurance policies for claims related to the PlayStation Network data breach. Zurich based its argument on the grounds that such claims “do not allege injury of damages covered under Coverage A—Bodily Injury of Property Damage Liability or Coverage B—Personal and Advertising Injury

Liability.”4

In this way, Zurich’s action for declaratory judgment posed not only an issue for Sony, the corporation liable for the breach, but also underscored a fundamental issue at the center of the e-commerce industry: the duty of insurers for privacy, internet and network liability. As seen in the case of Zurich’s 2011 action for Declaratory Judgment, insurers are increasingly willing to litigate the issue of whether commercial general liability policies provide insurance coverage for the theft of electronic data and harm to intangible property. Understandably, insurers are hesitant to indemnify corporations for data breach liability under many standard policies, due to the fact that the financial harm caused by a data breach is unpredictable and does not fall neatly within a defined policy coverage provision such as property damage, personal injury or bodily harm. In response to this evolving gap in coverage, many insurers have begun writing cyber-risk specific insurance policies to provide indemnity from liability for the unauthorized disclosure of sensitive consumer information.

The existence of cyber-risk insurance coverage, in and of itself, may not be enough to ensure that companies which compile sensitive consumer information adequately secure that electronic data as a matter of public policy. Accordingly, cyber-risk insurers face a moral hazard issue similar to traditional lines of property and causality insurance when underwriting adequately priced insurance premiums. As the costs resulting from a data breach continue to grow, firms with the greatest incentive to purchase insurance may be those with those with the greatest potential loss exposure, whether due to deficient

4 Id. at 12.
information security infrastructure or participation in a highly-regulated line of business.

Assuming that firms who seek to purchase cyber-risk insurance coverage possess a fixed budget for information security, highly priced cyber-risk insurance provides an incentive for firms to purchase indemnity from data breach costs without making a corresponding investment in the information security infrastructure necessary to protect consumer data. In the short term, this asymmetry between the insurer’s premium calculation and the insured’s level of care may lead to inadequately priced cyber-risk insurance coverage. Should an insured devote an outsized percentage of its yearly security budget to high-cost insurance plans over corresponding infrastructure investments, the insurance carrier will be exposing itself to an increased risk of loss over the long term.

If this is the case, higher policy premiums reduce the funds available for information security infrastructure investment, thereby creating a corresponding increase in future risk of loss for the insurer and by extension the consumer. Should an insured purchase a yearly claims-made cyber-risk policy that indemnifies the insured against state sanctions, administrative fines, property damage, business interruption and consumer lawsuits arising from a data breach, the insured possesses little incentive to sufficiently secure its sensitive consumer information at the level required by public policy.\(^5\) Thus, if the level of security infrastructure needed to price risk is lower than the level of infrastructure needed to adequately secure consumer data, firms with insufficient information security

\(^5\) J. Wylie Donald & Jennifer B. Strutt, Cybersecurity: Moving Toward a Standard of Care for the Board, 18 ELEC. COM. & L. REP. (BNA) 44, 2953 (2013) (discussing the ability of insurers to require the adoption of information security standards that fit the needs of a diverse range of business endeavors).
possess an incentive to invest in infrastructure only up to the level that is required to purchase insurance coverage rather than investing to the level that is adequate for consumer protection.

In this scenario, an insured that allocates budget to cyber-risk insurance coverage over annual investments in information security infrastructure becomes insulated from the legal liability arising from a data breach, at the expense of consumers whose information remains inadequately protected from third party theft and misuse. In this way, the moral hazard problem in cyber-risk insurance presents an important public policy concern, wherein an insured is able to offset their own liability for failure to adequately secure consumer information, while leaving consumers to contend with the financial fallout of the insured’s failure to adequately protect those same consumers’ personal data.

For the purposes of this Article the term “public policy” is not explicitly defined. The level of information security infrastructure that is needed to adequately protect consumer data as a matter of “public policy” is a normative debate and may depend on interrelated considerations including the scope and type of data insured. Accordingly, this Article does not seek to establish a single metric upon which to evaluate the efficacy of data protection infrastructure in all instances. Instead, this Article takes the position that data protection infrastructure is sufficient as a matter of “public policy” when a custodian of consumer data maintains infrastructure that reduces the likelihood of a security breach to minimum acceptable levels and retains only residual risk.

This Article seeks to address the problem of moral hazard in the cyber-risk insurance marketplace by proposing an independent, government funded information-sharing platform for insurers to anonymously pool historical loss data, claim histories, and compliance audits
of insureds in an effort to discount premiums for insureds that adequately secure consumer data at the level required for public policy. Similar to fire insurance and other property and casualty insurance lines, moral hazard in the cyber-risk insurance market can be mitigated by differentiated premiums based on discounts contingent on corresponding investments in information security infrastructure. Much in the same way that a physical storage facility may receive reduced premiums based on fire protections exceeding those required by building code regulations, so too can insurers predicate a corresponding reduction in cyber-risk policy premium on information security infrastructure benchmarks.

Developing these benchmarks as a technical matter will be challenging for insurers. Information security is a heterogeneous exercise across many lines of business. However, insurers may be in the best position to establish such a framework for information security benchmarks through the standard-setting and compliance functions of the insurance industry.6

By utilizing an information pooling system, insurers will be able to adjust premiums for firms that invest in information security infrastructure that reduces the insured’s risk of loss while simultaneously increasing the protections afforded to consumers. Accordingly, insurers party to the information sharing agreement will reduce their own risk of loss while creating an economic incentive for insureds to adequately secure consumer information. As a secondary effect, this information-sharing regime may serve to lower the cost of entry into the cyber-risk insurance marketplace, allowing additional insurance

6 TREAS. DEPT., SUMMARY REPORT TO THE PRESIDENT ON CYBERSECURITY INCENTIVES PURSUANT TO EXECUTIVE ORDER 13636 (2013).
companies to compete with current cyber-risk insurance carriers thereby creating a more competitive marketplace with a corresponding increase in risk adjustment and underwriting protocols with the end result of increasingly affordable cyber-risk insurance policies.

II. DEFINING CYBER-RISK

A. What Are Insurable Cyber-Risks?

E-commerce and online business are a defining economic characteristic of the modern era. While the risks borne by an entity doing business online are in some ways analogous to the traditional types of liability risks that many businesses’ face, some aspects of cyber-risk “are unique, in terms of location, degree, and visibility.”

Much in the same way that a brick-and-mortar storefront faces the risk of property damage and lost business in the course of a smash-and-grab robbery, so too do firms transacting business online. In the cyber-risk context, however, the perpetrator of the theft or property damage can commit their crime from the comfort of their home, thousands of miles away, thus challenging the application of traditional security measures.

Developing a comprehensive framework for analyzing an entity’s potential for cyber-risk losses depends heavily on the type of businesses in which that entity is engaged. The complete prevention of security breaches in an interconnected network may be impossible and in many cases, undesirable due to the diminishing rate of return of information security infrastructure investment.

8 Hulisi Ogut et al., *Cyber Insurance and IT Security Investment*: 
Accordingly, what makes cyber-risk management so unpredictable is the interdependency of cyber-risks among firms doing business within the marketplace.\(^9\) Because the security of consumer data relies on interdependent risks in a networked system, the information security risks which one firm faces will depend not only on that firm’s own security protocols but also the protocols of others with whom that firm’s network is linked.\(^10\) This phenomenon of a single security event in one insured’s system affecting that insureds peers—even if those peers are under different administrative control\(^11\)—has been called interdependent security risk.\(^12\)

In a networked system, externalities arise because of interdependencies between communicating computers.\(^13\) For example, should a malicious code breach an information security system through a compromised machine, that malicious code will have a lower barrier of entry to the other computers on that network, resulting in more damaged property and increased amounts of

---

*Impact of Interdependent Risk*, FOURTH WORKSHOP ECON. INFO. SEC. 1, 2 (2005), [http://infosecon.net/workshop/pdf/56.pdf](http://infosecon.net/workshop/pdf/56.pdf) (discussing the idea that complete prevention of security breaches is “technologically impossible” and in many instances would be undesirable because of the high costs and diminishing returns of security investments).

\(^9\) *Id.* (arguing that cyber-risk interdependence occurs in two ways: the physical link computers share via the internet and the logical interdependence that comes from the ubiquitous use of computer technology).


\(^11\) Jay P. Kesan et al., *Cyber-insurance as a Market-Based Solution to the Problem of Cybersecurity*, FOURTH WORKSHOP ECON. INFO. SEC. 1, 22 (2005), [http://infosecon.net/workshop/pdf/42.pdf](http://infosecon.net/workshop/pdf/42.pdf).

\(^12\) See Kunreuther & Heal, *supra* note 10.

\(^13\) Kesan et al, *supra* note 11, at 22.
compromised information. Thus, “this externality problem often results in a security investment’s private return that is lower that the social return.”

While the costs arising from any single data breach are unpredictable, the average total organizational cost of a data breach in the United States in 2013 was $5,403,644.00 or $188.00 per record. This amount is subject to variance, however, based on the industry that a breached entity is engaged in. On average, data breaches in highly regulated industries such as healthcare, finance and pharmaceuticals were more costly than data breaches in the energy, retail, and public service sectors.

Of this $5,403,644.00 average, the four primary cost centers of a data breach are: first, detection and discovery in the form of digital forensic investigations and audit services; second, escalation, including crisis management and communication to executive managers; third, notification costs in the pursuit of regulatory compliance; and finally ex-post response costs in the form of remediation activities, legal expenses and identity protection services for affected consumers. In addition to these process-related activities, affected companies may also experience opportunity costs associated with a security event in the form of turnover of existing customers and diminished future customer acquisition. In some case,
these lost business costs may even be more than any single one of the “process-related” expenses described above. In 2013, the average lost business cost for a United States organizations resulting from a data breach was $3,030,814.00.20

Financial institutions and health care providers possess a very high duty to protect consumer data residing on their networks and therefore a serious potential level of loss exposure. Firms that collect and retain such statutorily protected data must comply with internal controls and reporting standards set by the state and federal government. Even entities that are not specifically covered by laws or regulations pertaining to their specific industry are charged with a general duty to safeguard the consumer data under their control.21

In the insurance context, cyber-risk losses can be divided into two broad categories: first-party and third-party losses. First-party losses occur when an insured faces lost profits and expenses due to property damage (lost data, software, hardware) in addition to business interruption costs as the direct result of a data breach.22 Third-party losses, on the other hand, are losses that an insured incurs as a result of the damage caused, either directly or indirectly, to another firm or individual;23 these risks can include state and federal notification statute compliance, credit monitoring, administrative fines or penalties, and as seen in the Sony case, consumer lawsuits against the insured.

20 Id. at 18.
21 Kesan et al, supra note 11, at 9; see also 15 U.S.C. § 45(a) (2006) (FTC power to prohibit unfair or deceptive trade act which may include the protection of consumer custodial data).
22 Gordon et al, supra note 7, at 83.
23 Id.
B. Indemnifying Cyber-Risks through Insurance

Traditional insurance in the form of Commercial General Liability, excess umbrella, Errors & Omissions, and Directors & Officers policies often do not cover losses for non-physical property damage and electronic data. A review of traditional insurance policies demonstrates several gaps in coverage for potential cyber-risks. Among the most prominent of these gaps in traditional insurance policies for cyber-risk losses is the lack of a “trigger” provision that would create an insured occurrence in the event of a data breach. Furthermore, coverage for third-party losses related to unauthorized access to protected consumer information may not be covered, due to the fact that affected consumers are not named insureds under the insuring agreement. Geographical limitations on an insurance policy also compound the applicability of cyber-risk insurance coverage as the harm caused to an insured may originate outside of the insured area. Finally, and perhaps most important, insurers’ refusal to cover cyber-risk losses under traditional liability policies continues to drive companies toward cyber-risk specific insurance products.

With the development of the Internet-based economy, both federal and state governments have passed legislation to regulate the protection of nonpublic and personal consumer information. Laws such as the Health

---

24 Kesan et al, supra note 11, at 6.
26 Kesan et al, supra note 11, at 6.
Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, Executive Order 13636, state data breach notification statutes, and FTC consent decrees have sought to impose a higher standard of information security compliance upon firms that gather and preserve sensitive consumer data. As a result of these administrative burdens in conjunction with the increasing costs of data breach liability, insurers have begun offering products tailored to the specific risks associated with the data breach liability for many regulated industries.

Typically, cyber-risk policies provide coverage for both first-party and third-party losses. Generally speaking, first-party losses concern claims made by an insured for financial harm suffered directly by the insured organization as a result of an insured occurrence whereas third-party losses concern claims made against an insured, by a third-party, for losses related to an insured occurrence. In a data breach, an insured’s remediation costs for damage to property owned by the insured entity composes the bulk of a first-party loss while claims against the insured, made by third parties harmed as the result of a data breach, compose a preponderance of third-party losses.

<table>
<thead>
<tr>
<th>Insured First Party Losses</th>
<th>Insured Third Party Losses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property damage to intangible assets (e.g. software and electronic data)</td>
<td>Damage to third party property</td>
</tr>
<tr>
<td>Theft of proprietary information or consumer data(^\text{28})</td>
<td>Denial of access</td>
</tr>
<tr>
<td>Business interruption</td>
<td>Insufficient measures to protect a third party from viruses, system failure or programming errors</td>
</tr>
<tr>
<td>Damages to company assets caused by viruses</td>
<td>Unauthorized use of confidential information</td>
</tr>
<tr>
<td>Crisis management expenses</td>
<td>Loss of expected goods and services</td>
</tr>
<tr>
<td>Restoration expenses (e.g. restoring damaged software and replacing hardware)</td>
<td>Failure to prevent unauthorized access to, or use of, electronic or non-electronic data containing identity information(^\text{29})</td>
</tr>
<tr>
<td>Fraudulent transfer of money, securities, or other property</td>
<td>Defense expenses related to defending regulatory actions or third-party lawsuits</td>
</tr>
</tbody>
</table>

---


Categories of first-party claims that may be insured include: property damage to intangible assets such as software and electronic data; business interruption; the “theft of proprietary information or consumer data”\(^{30}\) that occurs as the result of “hackers (external and internal); viruses; extortion; programming errors; power surges and the like leading to network or system failure.”\(^{31}\)

Third-party claims may include a company’s liability for “damage to third party property consisting of intangible assets, namely software (programs) and data and or financial losses as a result of: denial of access, insufficient measures used to protect third-party from computer crime, spread of a computer virus, failure of software, and programming errors,” any or all of which lead to “network or system failures or loss of expected goods and services.”\(^{32}\) Additionally, third-party liability coverage can indemnify an insured from “intellectual property infringements encompassing software patents, copyrights, trade secrets, trade markets; defamation, libel and slander; invasion of privacy; unfair competition or false and misleading advertising; unauthorized use of confidential information.”\(^{33}\)

Beyond the financial benefit of absorbing information security losses, cyber-risk insurance provides a number of distinct advantages over government regulation as a means of encouraging adequate protection of consumer data. Unlike fines and sanctions levied by Attorneys General or government agencies on entities that do not comply with a minimum set of information security regulations, insurers can positively reinforce consumer data protection through financial incentives based upon different

\(^{30}\) Marsh, supra note 28, at 7.
\(^{31}\) Id.
\(^{32}\) Id.
\(^{33}\) Id.
classifications of risk. As a result of these financial incentives, information security infrastructure spending by an insured can be assessed on the basis of value added rather than the costs incurred. Assuming that an insurance carrier is able to perform an *ex-ante* risk assessment of an insured’s information security infrastructure, that insurer will be able to tie premiums to the level of the insured’s security. A moral hazard problem arises, however, in the event that an insured opts for greater (and more expensive) insurance coverage over a corresponding investment in security infrastructure.

III. MORAL HAZARD

A. Mitigating Moral Hazard in Traditional Insurance Lines

It is commonly noted that “protection from harm induces reckless behavior.” This phenomenon of increases in risky behavior, predicated on access to insurance, is known as moral hazard. Moral hazard is a systemic risk faced by all insurers. Generally, moral hazard consists of three categories of behaviors by insureds, all of which are unobservable by the insurer. The first type of

---

35 *Id.*
moral hazard, and the primary kind of behavior that this Article seeks to address, occurs when an insured takes less than optimal precautions against an insured risk. This particular behavior is referred to as ex-ante moral hazard and appears when an insured engages in a riskier activity than that insured would ordinarily undertake, on the basis of insurance coverage for the resulting loss. The second type of moral hazard, ex-post moral hazard, occurs when an insured makes insufficient efforts to minimize potential liability in the event of an insured occurrence due to insurance coverage for the resulting loss. The third type of moral hazard, sometimes defined as fraud, is an embellishment of losses by an insured to secure larger reimbursements under an insurance contract.

In all three of these cases, an insured externalizes the cost of their insurance claim to the insured risk pool. When an insurer is unable to distinguish between insureds which take proper precautions to mitigate ex-ante moral hazard liabilities and insureds which do not, the insurer is forced to charge a higher premium to all insureds, leading to cross-subsidization of socially undesirable behaviors.

On the front end of an insurance transaction, the insurer’s “most basic tool for creating incentives to reduce risk is the setting of differentiated premiums.” This may be accomplished in one of three ways. First, underwriting cyber-risks, similar to underwriting traditional property and casualty insurance lines, requires an insurer to obtain

\[\text{39 Id.}\]
\[\text{40 Id. (this type of behavior can be characterized as both ex-post moral hazard as well as fraud depending on the magnitude of losses embellished).}\]
\[\text{41 Id.}\]
\[\text{42 Id.}\]
\[\text{43 Omri Ben-Shahar & Kyle D. Logue, Outsourcing Regulation: How Insurance Reduces Moral Hazard, 111 Mich. L. Rev. 197, 205 (2012).}\]
detailed information regarding the risk characteristics presented by a particular insured. Information obtained during the underwriting process is strengthened by the use of verification methods in the form of yearly audits and/or on-site inspections to ensure that the information disclosed by an insured is accurate. The credibility of the underwriting process is further protected by “stiff sanctions on insureds who misrepresent information.”44

Second, under the McCarran-Ferguson Act’s exemption of insurers from federal antitrust law, insurance companies are allowed to pool and analyze risk-related information through a multitude of industry-owned risk rating agencies and bureaus. These information aggregation and sharing services assist in making insurance markets more stable and increasingly competitive by lowering the cost of entry into the insurance marketplace for insurers who would otherwise possess insufficient data to underwrite insurance coverage on their own. Thus, by sharing historical loss data and claims statistics, insurers are able to more effectively price risk, thereby ensuring stability in insurance markets.

Third, insurers who are privy to the information sharing schemes described above are able to alter underwriting protocols to modify premiums according to each policyholder’s individual risk assessment based on current behaviors, in addition to loss data over time.45

When underwriting individual property and casualty insurance policies, as opposed to group policies, “insurers can refine their premiums through the practice of ‘feature rating,’ in which they examine the insured’s individual risk

44 Id. at 206.
45 Id.
characteristics and adjust premiums accordingly.” 46 One example of this strategy from the property and casualty insurance context is the practice of discounting premiums for fire insurance, to more than offset the cost of added safety features, such as sprinklers and smoke detectors.

In addition to feature rating, insurers engage in “experience rating” by making “retroactive pricing adjustments or prospective pricing adjustments for future policy periods.” 47 The combined goal of experience and feature rating is to create insured-specific premium adjustments over time so that an insured is made aware of what safety investments correlate with particular reductions in anticipated claim costs – and by extension, corresponding reductions in premium. In this way, differentiated premiums can affect the level of safety investment made by an insured. “Insureds from whom the activity provides a high utility will purchase insurance” 48 and engage in the risk-reducing activity while “others from whom the activity provides only a low utility, will be priced out altogether.” 49

Beyond differentiated premiums, two common devices employed by insurers to mitigate moral hazard are deductibles and copayments. 50 Together, deductibles and copayments force an insured to bear a portion of any claims made under an insurance contract. For many years, moral hazard scholarship has acknowledged the tradeoff between

46 Id.
47 Id.
48 Id. at 207-8.
49 Id. at 208.
50 Romanosky, supra note 37, at 7.
“full insurance and optimal care incentives,” the idea being that the most efficient insurance contracts ought to require partial sharing of a loss between the insurer and insured.

While deductibles and copayments serve an important purpose in mitigating moral hazard in the insurance marketplace, neither is as efficient as “premium differentials in creating optimal incentives for the insured.” Thus, deductibles and copayments present less attractive incentive for insureds to mitigate losses, due to the fact that an insured does not enjoy the full social benefit of making the additional safety investment.

B. Moral Hazard in Cyber-Risk Insurance

As demonstrated above, differentiated premiums based on feature and experience risk-rating methodologies present arguably the most efficient method for mitigating ex-ante moral hazard in individual insurance policy contracts. In the cyber-risk context, however, ex-ante moral hazard presents an additional public policy concern wherein an insurer is subject to increased liability in the form of additional consumer harm. For example, should an insured inadequately secure consumer data, an insurer may be liable not only for property damage remediation losses incurred by an insured but also for the legal liability arising from the insured’s unauthorized exposure of statutorily

51 Ben-Shahar & Logue, supra note 43, at 208-9. See generally Steven Shavell, On Moral Hazard and Insurance, 93 Q. J. Econ. 541, 546 (1979) (discussing the advantage of incentive effects to purchase insurance, where the low cost of obtaining partial insurance coverage will outweigh the imposition of risk).

52 Ben-Shahar & Logue, supra note 43, at 209.

53 Id.
protected consumer data.

In this way, \textit{ex-ante} moral hazard in the cyber-risk marketplace presents an important concern for consumers. If an entity that invests primarily in cyber-risk insurance products rather than information security infrastructure is able to offset data breach liability for the resulting consumer harm, that entity possesses little incentive to pursue additional investments in security infrastructure, thereby creating both an increased risk of loss for the insurer as well as an increased risk of harm to the consumers.\footnote{While this Article does not specifically address the reputational harms that a breached entity may face as the result of unauthorized access to consumer data, it is important to note that both statutory data breach notification compliance and cyber-risk claim reporting carry inherent reputational risks for the breached entity. By publicly reporting a data breach, an organization risks economic harm in the form on diminished future customer acquisition in addition to reduced consumer confidence in the organization itself. For a more detailed analysis of how such secondary loss exposure may affect an insured’s behavior when reporting data breach incidences to insurers, see Tribid Bandyopadhyay et al., \textit{Why IT Managers Don’t Go for Cyber-Insurance Products}, 52 COMMUNICATIONS OF THE ACM 68 (2009).}

Hence, a cyber-risk insurance policy which indemnifies an insured (who does not adequately secure consumer data) from the liability arising out of unauthorized access to that data will create an incentive for an insured to retain only the level of information security infrastructure needed to purchase insurance coverage sufficient to offset their own potential liability without ensuring additional consumer protection. Assuming that a company which seeks to purchase cyber-risk insurance possesses a fixed yearly budget for information security investments (both insurance and infrastructure) and assuming that the level of information security infrastructure required for an insurer to adequately price
risk is lower than the level of infrastructure required to adequately secure consumer data, a rational purchaser will invest in infrastructure only up to the point of obtaining insurance coverage to the detriment of the consumer. Thus, an insured’s reliance on insurance coverage rather than infrastructure investment may insulate an insured from the legal liability resulting from a data breach, while simultaneously leaving consumers to deal with the financial and administrative fallout of that insured’s risky behavior.

At present, cyber-risk insurance is hampered in this regard by a number of practical and unresolved research challenges related to underwriting cyber-risk coverage. One of the most prominent of these challenges is the information asymmetry between the insured and insurer.55 Because an insurer underwriting cyber-risk coverage possesses finite resources to monitor an insured’s actions that affect the probability of loss after an insurance contract has been signed, it may be difficult to determine whether an insured has engaged in behaviors that increased the likelihood of a covered loss. Examples of some behaviors by an insured which may create additional risk of loss to the insurer include: “vital information regarding applications, software products installed by internet users, and security maintenance habits, which correlate to the risk types of users.”56

Of the current cyber-risk insurance policies available, many incorporate provisions which are designed to address potential moral hazard problems.57 One example of such a provision states that an insured “cannot claim

56 Id.
57 Kesan et al, supra note 11, at 14.
payment for a loss or claim associated with failure to take reasonable actions to maintain and improve their security.” While such a provision provides sound protection for the insurer from an insured’s failure to mitigate *ex-ante* moral hazard, the coverage exclusion may not sufficiently address consumer harms resulting from a data breach other than to place the *onus* of the resulting loss upon the insured rather than the insurer. For example, if an insured suffers a data breach after failing to update critical infrastructure software, the insurer may dispute coverage but the affected consumers have still suffered harm. For this reason, other methods such as heightened self-retained policy limits and/or deductibles may serve to encourage “self-protection,” in light of the fact that self-insurance and market insurance can “both redistribute income toward hazardous states.” Accordingly, tying a firm’s insurance premiums to that firm’s investment in self-protection may help to mitigate moral hazard. If an insured’s level of information security infrastructure can be observed by the insurer on an *ex ante* basis, the presence of cyber-risk insurance may increase the amount an insured spends on self-protection as an economically rational response to the corresponding reduction in insurance premiums.

At its heart, the fundamental problem of *ex-ante* moral hazard in cyber-risk insurance rests upon the fact that an insured may be able to achieve sufficient information security infrastructure to purchase cyber-risk insurance without first obtaining the level of protection needed to

58 Id.
59 See id. at 20 (discussing insurance, self-protection, and complements, where the insurer can observe the level of protection of the insured and price is negatively related to the amount of self-protection).
adequately secure consumer data. Assuming that the level of security required for adequate protection of consumer custodial data as a matter of public policy is greater than the cost of the information security infrastructure necessary for insurers to properly price risk, an insured will possess an incentive to retain only the level of infrastructure that is required to obtain coverage which indemnifies that insured from data breach liability. Thus, the infrastructure cost of achieving sufficient consumer data protection may be greater than the cost of obtaining insurance coverage for indemnification of data breach liability, resulting in an ex-ante moral hazard issue with direct consequences for consumers.

IV. INSURANCE REGULATION & INFORMATION SHARING

A. Information Sharing Under the McCarran-Ferguson Act

Federal antitrust law historically has curtailed the extent to which private corporations are legally allowed to share information regarding the costs and profits of their business. Traditionally, sharing of information between competitors has led to cartelization and decreased competition within a competitive marketplace. Insurance, however, poses a unique problem when subject to federal antitrust law, as insurance itself is neither a traditional area of private enterprise in which “unrestrained capitalist rivalry ought to prevail,”62 nor is it a purely public utility with monopoly privileges subject to “rigid rate-making.”63

63 Id.
Instead, insurance has been described as a business “clothed in a public interest,”\(^\text{64}\) which affects the community at large and therefore requires regulation that is not traditionally employed for private enterprise businesses.

Historically, the authority to regulate information sharing among insurers has been a product of state law. Insurance regulation is unique in the sense that very few areas of law expressly assign the states’ supervisory power over commerce in the same way that the McCarran-Ferguson Act does for insurance regulation. Broadly, the extent to which a state may regulate the insurers doing business within its jurisdiction — the “business of insurance” — is fundamentally tied to the sovereign power of the state itself. Each state, with the assistance of the National Association of Insurance Commissioners, sets the legal regulations specifying how insurers may legally share claims costs and historic loss data without running afoul of each state’s antitrust laws. This section begins with a brief overview of court cases and decisions leading up to the McCarran-Ferguson Act’s antitrust exemptions for insurers, and seeks to illuminate the types of information sharing platforms that insurers utilize under both state and federal law.

Today, insurance continues to be primarily regulated by states. The McCarran-Ferguson Act of 1945 provides that state regulation and taxation of the insurance industry best serves the public interest and that no federal law shall be “construed to invalidate, impair or supersede any law enacted by any state for the purpose of regulation the business of insurance.”\(^\text{65}\) In this way, the insurance industry has been exempted from the Sherman, Clayton,

\(\text{64}\) Bentley v. Allstate Ins. Co. 227 Ga. 708, 709 (1971).
and Federal Trade Commission Acts, applicable to the extent that the so-called “business of insurance” is not regulated under the laws of the several states.

Section 2 of the McCarran-Ferguson Act specifies the criteria to be used in determining whether an insurer’s activity falls within the scope of the antitrust exemption afforded to insurance companies generally. Section 2 of the Act states in part that if an activity is within the “business of insurance,” that activity will be exempt from federal antitrust law. While precisely what constitutes the “business of insurance” may be an undefined and ambiguous term under the McCarran-Ferguson Act, the Supreme Court has crafted a three-prong test for determining whether an activity of an insurer falls within the “business of insurance.”

Because insurance is regulated at the state level, many states have differing interpretations as to what the “business of insurance” entails. One reading of the McCarran-Ferguson Act’s exemption for insurers from federal antitrust law might include all activities that are “regularly conducted by those firms which have as their principal purpose and effect the passage of risk from one party to another.” A broad interpretation such as this may include any transaction which assists in the passage of risk from one party to another, even third parties such as insurance agents, brokers, and information aggregation services within the business of insurance. Currently,

---

67 Id.
68 Id. at 89.
however, this patchwork of state regulation has largely been supplanted by NAIC Model Acts, draft laws suggesting how states ought to regulate insurance companies within their jurisdiction.

In antitrust case law, courts have tended to favor a view that federal antitrust laws are displaced by state regulation when state laws regulate the same conduct that federal antitrust law seeks to control.\textsuperscript{70} Perhaps the clearest case of a federal antitrust act exemption for insurers comes from plenary rate-setting in states which require insurance premium rates to be filed with the Insurance Commissioner before an insurer can issue policies within that jurisdiction. The strongest argument for an antitrust exemption for insurance companies, however, is that such an exemption facilitates economically efficient sharing of information thereby permitting insurers to evaluate and price risk more effectively.\textsuperscript{71}

Cooperation between insurance companies is necessary to achieve accurate risk pricing within the industry.\textsuperscript{72} Proper evaluation of risk requires extensive sampling of past occurrences as well as analysis of sample data to predict future losses. Without information sharing, each insurer would underwrite coverage based on only its own historical loss data, making accurate underwriting nearly impossible for all but the largest and oldest insurers. Furthermore, collaboration in the form of information sharing also achieves economies of scale, as an industry-rating bureau can perform the data sampling and analysis used by all insurance firms underwriting a certain type of risk, thereby reducing the cost of acquiring information for all insurers within a particular jurisdiction or line of

\textsuperscript{70} Id. at 28.
\textsuperscript{71} Id. at 47.
\textsuperscript{72} Id. at 48.
business.

“The strength of this argument for information sharing depends substantially on the type of information that is being shared.”\textsuperscript{73} In the past, ratings bureaus have provided three general types of information to the insurance industry: historical loss costs, prospective loss costs, and advisory rates. Thus, the argument for information sharing among insurers centers on the transaction costs associated with antitrust regulation. Were an independent third party to purchase loss data from multiple insurers, then analyze, compile and sell that data on the annual results of specific insurance lines back to the insurers, the transaction costs associated with such a system would be higher than if insurers were allowed to directly share information among themselves.

Accordingly, collective investment in shared information produces economic efficiency in the insurance industry. If information sharing were prohibited, numerous inefficiencies would arise. Pooling and sharing loss data is efficient because it treats information as a public good: that is, the use of information by one firm does not preclude the use of the same information by another. Given expenditures for information, increased access to loss data ensures that premiums will more accurately reflect the aggregate information that all firms share, thus avoiding replication of information expenditures and keeping costs low.\textsuperscript{74} Furthermore, a decrease in the ability to share claims data will result in firms using less information to set premium rates, thereby exacerbating adverse selection problems caused by informational asymmetry in the insurance industry.

\textsuperscript{73} Id. at 49.

\textsuperscript{74} Ralph A. Winter, \textit{The Liability Crisis and the Dynamics of Competitive Insurance Markets}, 5 \textit{YALE J. ON REG.} 455, 497 (1988).
marketplace. Finally, the cost of information in the insurance industry is fixed and any reduction in access to information for rate setting purposes would affect smaller firms more adversely than larger firms, increasing the market concentration, and resulting in a less competitive insurance market.\footnote{Id. at 498.}

In some states, the Department of Insurance designates a State Rating Bureau to serve as a consumer representative in hearings related to the appropriateness of insurance premium rates. The State Rating Bureau “collects and analyzes statistical data in order to provide technical advice to the Commissioner on oversight of auto, workers’ compensation, health and other insurance markets.”\footnote{Office of Consumer Affairs & Business Regulation, State Rating Bureau, http://www.mass.gov/ocabr/government/oca-agencies/doi-lp/doi-departments/state-rating-bureau.html (last visited Mar. 17, 2014).} In addition to State Rating Bureaus, the NAIC model acts also allow for “Insurance Support Organizations” which are organizations that collect loss data and claim costs from insurers “for the purpose of providing the information to an insurance institution or agent for insurance transactions.”\footnote{Nat’l Assc. Ins. Comm’rs, NAIC Ins. Info. & Privacy Prot. Model Act § 2(M) (1992).} Examples of some well-known Insurance Support Services are: A.M. Best, ISO – the Insurance Services Office, and CLUE – the Comprehensive Loss Underwriting Exchange.

The NAIC’s Insurance Information and Privacy Protection Model Act establishes “standards for the collection, use and disclosure of information gathered in connection with insurance transactions by insurance institutions, agents or insurance support organizations.”\footnote{Nat’l Assc. Ins. Comm’rs, NAIC Ins. Info. & Privacy Prot. Model Act Preamble (1992).}
Insurers are then able to request reports from Insurance Support Organizations and use the historical loss data, projected future claim costs and advisory rates in their own underwriting, decision-making, and strategies. Historically, Insurance Support Organizations have been the predominant way in which insurers pool information without running afoul of state law. More recently, however, a federal alternative to the NAIC’s Insurance Support Organization information-sharing regime has been proposed in the context of health data collected by recipients of Veterans Benefits, Medicare and Medicaid.

B. Information Sharing and the Federal Government

The Affordable Care Act proposed a number of new incentives and methods for health insurers to share information in ways that substantially differ from the Insurance Support Organization and state rating bureau information collection methodologies. The Centers for Medicare and Medicaid Services are tasked with establishing a national program that collaborates with treating physicians across care settings, aggregating data and sharing information regarding managed health care cost and quality. According to this proposal, Medicare beneficiaries will be eligible to have their claims data shared among industry participants to better serve beneficiaries. This system, proposed at the federal level, offers an alternative to the state level information-sharing platform currently in place.

Such a system of information sharing, regulated by

79 New ACO Proposed Rule: Shared Data Could Lead to Privacy, Security Concerns for Participants, 10 No. 4 GUIDE TO MED. PRIVACY & HIPAA NEWSL. 4, May 2011.
the federal government and authorized under the Affordable Care Act, provides a new way for government and physicians to pool claims data to positively affect a public policy concern. 42 CFR Part 425 proposed the Medicare Shared Savings Program: Accountable Care Organizations. This proposed rule implements § 3022 of the Affordable Care Act and relates to payment of providers participating in Accountable Care Organizations (“ACOs.”) It relies on the participation of ACOs in the Shared Savings Program to report claim data and receive feedback from healthcare providers. While such a program is quite dissimilar to the Insurance Support Organization and State Rating Bureau methods detailed above, a federal information-sharing platform possesses some unique advantages unavailable to Insurance Support Organizations and state rating bureaus.

In addition to the Affordable Care Act, the Health Information Technology for Economic and Clinical Health Act (“HITECH”) has encouraged healthcare providers to move to electronic health record-keeping systems. 80 The benefits of the HITECH Act include: quicker and more accurate patient information availability, enabling healthcare providers to more easily spot possible health problems; the easy sharing of information among doctors, hospitals and systems, thereby allowing better coordination of care; and increased patient engagement, allowing patients and families to view their own health information. 81 Perhaps most importantly, the HITECH Act provides federal grants to assist states in developing Health Information Exchanges (“HIEs.”) 82 These HIEs are intended to capitalize on the ease of access and efficiency

81 Id. at 860.
82 Id.
conditions that the electronic medical records provide, as outlined above.

In the healthcare context, a national network of aggregate claims data for rate-calculation may be preferable to Insurance Support Organizations and state rating bureaus due to the fact that a centralized risk adjustment agency can better ensure the integrity and consistency of statistical data and reporting among competing insurance companies.\(^83\) If data from one ACO beneficiary population demonstrates high rates of hospital readmission, that ACO can consider actions to improve discharge coordination among attendant physicians. In the same way, if an HIE is able to determine that a particular set of health care providers in one state’s jurisdiction are responsible for inefficient or even negligent medical care, the HIE may be able to identify those concerns more quickly than previously possible.

While the implications of such a federal information sharing system have not yet been fully explored, these systems present a viable alternative to State and Insurance Support Organization information sharing. From a regulatory standpoint, a single government agency or contractor will be able to centralize risk adjustment as well as ensure the integrity of claim data and risk scoring among competing insurers.\(^84\) Similar to the “economies of scale” argument for insurance support organizations and rating bureaus, a federally centralized system of insurance loss data and claim costs avoids duplicative reporting, collection expenses, and storage expenses.

Arguments against a government agency or

---


\(^{84}\) *Id.*
contractor for risk calculation and data collection, however, focus primarily on the concerns of insurance companies. Should a government data collection or risk-scoring algorithm inaccurately predict current or future claim costs, insurers may lose profits in the risk-adjustment process.\textsuperscript{85} Thus, maintaining the trust of insurance companies that agree to a government sponsored information sharing and risk-calculation program will be of the utmost importance.

V. \textbf{HOW INFORMATION SHARING MITIGATES MORAL HAZARD}

A. Economic Efficiency of Information Sharing

The leading argument for information sharing among insurers is that a federal antitrust exemption facilitates an economically beneficial exchange of information by permitting insurance companies to better evaluate risk and thereby to price premiums more accurately.\textsuperscript{86} Despite concerns regarding the potential anticompetitive and price-fixing effects of information sharing among insurers, the social cost of information sharing’s reduction in competition within the insurance marketplace is outweighed by the net benefit of more accurately priced insurance premiums, resulting in more insurers competing for the same business.\textsuperscript{87}

Any argument which favors information sharing among insurers begins with the basic observation that faulty pricing of insurance products causes harmful economic distortions and inefficiencies in the insurance marketplace. When rates are set too low, harmful behavior by an insured is subsidized through insurance coverage,

\textsuperscript{85} \textit{Id.}
\textsuperscript{86} Macey \& Miller, \textit{supra} note 69, at 47.
\textsuperscript{87} \textit{Id.} at 48.
resulting in a social burden.\textsuperscript{88} Furthermore, excessively low premium rates may result in some firms leaving the insurance industry, thereby creating a residual market wherein many parties who desire insurance find themselves unable to obtain insurance coverage at all.

Conversely, if premium rates are set too high, insurance firms will profit while policyholders pay too much, causing the socially desirable activity that insurance incentivizes to be discouraged. A secondary effect of excessive premiums is that some consumers will be unable to afford insurance at all and will be forced to either self-insure or to cease the activity for which they desire insurance coverage. Finally, high premium rates reduce insurers’ incentives to operate efficiently, as the regulated pricing environment of shared loss data forces insurers to resolve claims at a level of efficiency that is beneficial to both the company and the policyholder.\textsuperscript{89}

Thus, cooperation between insurance companies facilitates the accurate pricing of risk within the insurance industry.\textsuperscript{90} Achieving proper evaluation of risk requires extensive sampling of past occurrences as well as analysis of sample data to predict future losses. When insurers are unable to share loss data, companies are forced to rely solely on historical data they have collected. Such a rule effectively denies smaller insurers the benefits of actuarially sound loss data for ratemaking purposes.\textsuperscript{91} It then follows that smaller insurers would be unable to set adequate or competitive premium rates, meaning those

\begin{flushright}
\textsuperscript{88} Id.
\textsuperscript{89} Id.
\textsuperscript{90} Id.
\end{flushright}
small insurers risk insolvency or being priced out of the insurance market altogether. Thus, the inability to share data would not only reduce the level of competing companies within the insurance marketplace but may also harm the policyholders of smaller insurance companies that are driven to insolvency.\footnote{Id.}

Of course, evaluation of past occurrences and historical losses can only occur if insurers are willing to share claim data with one another. Information sharing services provide two important functions within the insurance industry. First, information sharing “makes historical loss data available in a sufficiently large sample to provide a high degree of statistic reliability in the analysis.”\footnote{Macey & Miller, supra note 69, at 48.} Second, cooperation in the form of loss information sharing achieves economies of scale. The arguments for sharing information within the insurance industry are most persuasive, however, when applied to property and casualty insurance lines where the economic justifications for sharing loss data extend beyond historical claims.\footnote{Id. at 49.}

Information sharing among competing insurance companies creates a public benefit by ensuring the accurate assessment of insurance premiums within the industry.\footnote{Id. at 48 (discussing the need for accurate assessment of insurance premiums especially in property and casualty insurance lines).} Because the price of insurance premiums reflects an insurer’s “evaluation of the probable costs of paying claims, as well as the other costs of doing business and a reasonable provision for profit,”\footnote{Id.} knowledge of historical claims data is of the utmost importance for predicting the costs of future losses in property and casualty lines. For
many insurance companies with insufficient data, however, the cost of future payable claims may be difficult to assess at the time that an insurance policy is written. Therefore, a proper evaluation of downstream risk must include the “sampling of past occurrences of [the] event insured against, as well as analysis of the historical sample in order predict losses in the future.”

Data collection services in the form of insurance rating bureaus typically provide insurers with advisory rates and historical loss data in addition to prospective loss analyses to project the cost of future claims. This makes the data collection function of insurance rating bureaus important for three reasons. First, prospective loss analysis utilizes information sharing to estimate the future cost of claims made on past loss data. Second, trend analysis takes into account the economic and legal changes, which may affect the future cost of claims and forecasts future losses based on information that historical loss data alone may be unable to predict. Finally, the dissemination of historical and projected loss data through insurance rating bureaus achieves economies of scale by performing the data sampling and analysis functions for all insurance companies underwriting a certain type of coverage, thereby reducing the cost of acquiring information for all insurers within in particular jurisdiction and or line of business.

Therefore, collective investment in shared information is economically efficient within the insurance industry. If information sharing were prohibited, numerous inefficiencies would arise. Pooling and sharing loss data is efficient because it treats information as a public good, as

---

97 Id.
98 Id. at 50.
99 Id. at 48.
the use of information by one firm does not preclude the use of the same information by another. Given expenditures for information, increased access to loss data ensures that premiums will more accurately reflect the aggregate information that all firms share, thus avoiding replication of information expenditures and keeping costs low.\textsuperscript{100} Second, a decrease in the ability to share claims data will result in firms using less information to set premium rates, thereby exacerbating adverse selection problems caused by informational asymmetry in the insurance marketplace. Finally, the cost of information in the insurance industry is fixed and any reduction in access to information for rate setting would affect smaller firms more adversely than larger firms, increasing the market concentration, and resulting in a less competitive insurance market.\textsuperscript{101}

B. Information Sharing to Mitigate Consumer Harm in Cyber-Risk Insurance

As outlined above, differentiated-premium based risk-adjustment and information sharing are two of the primary ways in which insurers are able to provide adequately priced polices to consumers. In the formation of an insurance contract, information flows between both the insurer and insured.\textsuperscript{102} Ideally, each party supplies information regarding the factors of risks that affect the insurability of the would-be-consumer.\textsuperscript{103} In traditional fire insurance, a company with smoke detector and sprinkler systems that hopes to purchase a fire insurance policy will be eligible for a lower-cost premium based on the

\textsuperscript{100} Winter, \textit{supra} note 74, at 497.
\textsuperscript{101} Id. 498.
\textsuperscript{103} Id.
composite knowledge of the insurance industry that sprinkler systems reduce the likelihood of fire losses and therefore warrant a corresponding reduction in premium.\(^{104}\) Most importantly, this sharing of information from insurer to insured gives the insurance consumers a financial incentive to achieve reduced risk of loss based on the collective experience of the insurance industry.

In the cyber-risk insurance context, however, the financial incentive to bolster security infrastructure in order to reduce the likelihood of loss achieves a consumer protection goal beyond that raised by fire insurance alone. If an insured possesses a financial incentive to invest in additional information security infrastructure in the form of a reduced policy premium, the insurer will be able to reduce its own likelihood of future loss while the non-party consumer, whose data is stored by the insured, benefits from the increased protection of the insured’s additional information security investments.

Unlike fire insurance or other traditional lines of property and casualty insurance, one of the most prominent issues in underwriting cyber-risk coverage is the lack of information regarding frequency, magnitude, and claim costs of both actual and potential data breach incidents.\(^{105}\) Carriers may be reluctant to share information among one another—or with the government—due to the fact that additional reputational risks may follow any disclosure of a company’s data breach claim expenses. Thus, if an independent body were created for insurers to anonymously share information regarding data breaches claim costs, the

\(^{104}\) Id.

insurance industry may then be able to offer increasingly industry-specific cyber-risk products that are priced precisely for the levels and types of risk which they cover.

This Article proposes creating an independent, government-sponsored cyber-risk service bureau to collect claims and loss data, identify effective information security measures, and promote the development of increasingly accurate premium rates that will “reward” companies which choose to invest in security infrastructure that adequately protects consumer custodial data as a matter of public good. In this way, a cyber-risk rating bureau creates a market-based incentive to adopt security protocols that permit risk managers to trade off infrastructure investments with insurance premium reductions, thus lowering the cost of a cyber-risk loss for an insured while simultaneously reducing the likelihood and magnitude of those losses for the insurer. By allowing insurers to anonymously share loss data, and by requiring those insurers who do share such data to issue corresponding reductions in premium based on experience-rating adjustments for security metrics that reduce the risk of harm to consumers, insurers will be able to encourage data protection sufficient for public policy.

If cyber-risk insurance carriers are able to rate an insured’s cyber-risk policy premiums based on that insured’s continuing investments in information security infrastructure, insurers will occupy a unique space in the information security market, with the ability to create a market-based incentive for information security metrics that adequately secure consumer data. In this way, insurers may be in a better position than legislatures and government agencies to promulgate standards which serve to protect not only the financial interests of the risk-bearing insurer but also the consumers who have personal information stored by the insured. Thus, a cyber-risk rating bureau will aid this function of cyber-risk insurance by promoting higher levels of security investments, increasing
the overall levels of safety for information security infrastructure; facilitating standards for best practices to reduce consumer harm as cyber-risk insurance carriers benchmark proper security levels for risk management and consumer protection decision making,\textsuperscript{106} and creating an insurance market that results in a greater net social benefit than government regulation alone could produce.\textsuperscript{107}

Based on the assumptions outlined in § III.B of this Article, the level of information security infrastructure which a firm needs to retain in order for an insurer to accurately price cyber-risk coverage may be lower than the level of infrastructure needed to adequately protect the consumer information which that firm stores. If this is the case, and insurers writing cyber-risk coverage indemnify an insured for liability resulting from the exposure of protected consumer data, both insurers and consumers will be subject to increased levels of financial harm if an insured chooses to allocate information security funds primarily to insurance coverage rather than to security infrastructure. A cyber-risk rating bureau accomplishes this, and corrects this market failure, by allowing cyber-risk insurance carriers to share information which precisely

\textsuperscript{106} Kesan et al, supra note 11, at 35.

\textsuperscript{107} There is a potential for industry capture of any risk rating organization, and a cyber risk rating system should contain a safeguard mechanism to properly serve the interests of both consumers and insurers. The safeguard’s purpose would be to ensure that the process of cyber-risk rating itself does not become a function of the industry, subject to the external pressures of the marketplace, and independent of the insured risk. A detailed analysis of how such a safeguard would operate in practice not presented here, but for an analysis and proposal addressing this problem in the mortgage lending context see Jeffrey Manns, \textit{Rating Risk after the Subprime Mortgage Crisis: A User Fee Approach for Rating Agency Accountability}, 87 N.C. L. REV. 1011 (2009).
addresses the relevant risks presented by each insured when underwriting policies. Thus, the availability of loss data and rate-setting information available to insurers through the cyber-risk rating bureau encourages insureds to allocate optimal levels of investment toward infrastructure rather than relying on insurance coverage to offset data breach losses, to the benefit of both the insurer and the consumer.

VI. CONCLUSION

The expansion of the cyber-risk insurance market is likely to continue in the coming years. While the gross written premiums for cyber-risk insurance policies currently stand at the $1 billion dollar mark (up from $800 million in 2011) the cyber-risk insurance market still represents only a tiny fraction of the $247 billion in total direct premiums written in the United States commercial insurance lines market for 2012.108 As insurers continue to limit cyber-risk coverage under existing policy lines, insurance carriers will be able to move insureds towards comprehensive cyber-risk-specific insurance plans, establishing consistent standards and best practices that improve the ability of insurers to price coverage and underwrite insurance. This Article recommends a government sponsored but independent cyber-risk rating bureau to assist insurers and benefit consumers through the sharing of historical loss data, claim costs, and projected future claims in order to ensure the accuracy of cyber-risk coverage pricing and to reward the adoption of security standards that benefit consumers. In this way, insurers may

be able to implement safety standards to encourage
consumer protection of electronic data in the rapidly
evolving landscape of information security’s diverse risk
sectors in a manner that government regulation alone is
unable to achieve.109

109 Donald & Strutt, supra note 5, at 2953.
The Deregulation and Swarming of Cyberwarfare: The Need for and Limitations of Law in Enabling Aggressive ‘Hacking-back’ and Pre-Emption

By Dr. Mils Hills

Abstract:

This conceptual paper seeks to add some critical tone and shades of light and darkness to the considerations associated with ‘hacking-back’ by liberal democratic states. As with counter-insurgency and related operations, the challenges are that whilst state and non-state adversaries may not play by our rules, we will stick to ours. What space does that leave, then, in an era of unrestricted warfare, for aggressive cyber counter-strike and pre-emptive activities? In summary, the need for creativity and innovation should allow the development of tools, tactics and strategy that deliver strategic competitive advantage, cognizant of legal and other controls, constrains and frameworks. As part of a developing pipeline of research conducted at Northampton Business School, UK, the author draws on consultancy and support to elite military units in the UK, those who develop doctrine, concepts and force for the British Army and relevant security organizations in the UK and beyond.

1 Associate Professor of Risk, Resilience and Corporate Security, Value-Chain Research Group (VCRG), Northampton Business School, University of Northampton, UK mils.hills@northampton.ac.uk.
I. INTRODUCTION

This paper sets out the context in which liberal democratic states need to be able to draw on an inarguable legal mandate to both respond and pre-empt electronic attacks or attacks on their electronic infrastructure.\(^2\)

In an era of unrestricted warfare, where tools and skills are ever more widely available; where states have lost the monopoly on the use of lethal violence on literal battlefields, and can no longer realistically be said to have the exclusive license to use electronic lethal violence; where our businesses, media, health and other infrastructures may be the (un)intended targets of cyberwarfare; and, perhaps most troublingly, where attacks may well be mounted by those who swarm from a global constituency to actively contribute to a cause, we are faced with a great lack of guidance as to what constitutes an appropriate and legally defensible response. The context is of an acute challenge posed by the ease of swarm activation - intentionally mounted by hostile states, activist groups or movements or unintentionally when individuals or groups feel the need to add their support to a cause which energizes them.

How can international and domestic, military and civil law prepare for the challenge of ‘hacking back’\(^3\) in this swamp of swarmed activists,\(^4\) hostile states and others

\(^2\) This paper is written from the perspective of a non-legal scholar, dimly aware of some of the provisions of the Laws of Armed Conflict (LOAC).
\(^3\) See generally KENNETH E. HIMMA, INTERNET SECURITY: HACKING, COUNTERHACKING, AND SOCIETY 99 (2007) (surveying recent ethical policy issues having to do with the Internet and cybersecurity).
joining the melee? When anyone with a grudge, cause or preoccupation can throw their hat into the ring, take up electronic arms and cleave to the fray, states must anticipate difficult and challenging times ahead. Given the challenge posed by such a swarm, pre-emptive activity by states to disrupt any calls to action, distribute toolkits, and teach skills, etc., could be a beneficial means of risk reduction when a swarm-activation event arises.

Grounded in an appreciation of the need for liberal democratic states to sustain National Strategic Competitive Advantage\(^5\) – as well as enabling the competitive advantage of businesses hosted in our liberal democratic states (who also operate in other jurisdictions) – this paper aims to contribute to law- and policy-makers’ thinking in this challenging area. A key conclusion is that law is going to offer little in terms of a panacea to the volume, vectors and velocity of cyberwarfare attacks – a context where attribution may not meet conventional evidential standards and the necessity for counter-strike may be a matter of existential survival rather than ideological or political choice.

II. THE CHALLENGE FOR LIBERAL DEMOCRATIC STATES, THEIR MILITARIES, AND THEIR SECURITY SERVICES

Cyberwarfare was surely never meant to be like this. The barriers to entry are often so low (specifically: time to self-educate is the primary necessity, rewarding the time-rich and cash-poor) and the likelihood of capture and/or punitive measures remains so slight that almost anyone can and does become involved, whether as hacker, malware designer or (one anticipates) even the targeter of electronic networks via physical destruction or degradation.\(^6\) Warfare and the employment of lethal violence was – once and for a while – the preserve of state-sanctioned militaries. Cyberwarfare – along with compressing time and space – has collapsed distinctions between adversaries and frontlines.\(^7\) As this paper goes to press, Syria has become the latest failing state context to form a more-or-less open playground for a global community of mobile individuals to travel to and undertake whatever forms of violence they care to pursue.

Although reprehensible and revolting as this certainly is, the same phenomenon of self-recruitment to, and action in pursuit of, an adopted cause is seen in the cyber-domain. The electronic front line is everywhere and nowhere all at once. One can become energized to an

---


agenda and choose to do something about it at any time.\textsuperscript{8} I have written elsewhere about how we might explore and challenge the dynamics of such self-recruitment.\textsuperscript{9} However, this is not a situation that is likely to change. Indeed, one might argue that it is likely to become considerably more challenging.

For example, just as the collapsed state of Syria now faces the unofficial ‘free for all’ in which anyone is able to enter, join a militia, receive some basic weapons or explosives training and become part of the fray, those charged with countering cyber-warfare and attending to the legal frameworks under which any pre-emption or response would be constructed face equally acute problems. Some states are reacting to the problem of their citizens fighting in the Syrian conflict by threatening to withdraw citizenship.

Can the same principle – buttressed by labelling the activity as terrorism – apply to those who undertake e-terrorism, either deliberately under the flag of a foreign regime, recruited by such a regime, crowd-sourced by outrage at some cause or another, or from some other motivation?\textsuperscript{10} What needs to be done about those of our

\textsuperscript{8} See Dorothy Denning, \textit{Cyberwarriors: Activists and Terrorists Turn to Cyberspace}, XXIII, 2 HARVARD INT’L REV., 70, 70-75 (2001) (using the Palestinian-Israeli conflict of late 2000, which involved hacking attacks, to illustrate the growing use of cyberspace as a digital battleground).


\textsuperscript{10} See Mark Manion & Abby Goodrum, \textit{Terrorism or civil disobedience: toward a hacktivist ethic}, 30, 2 ACM SIGCAS COMPUTERS & SOC’Y, 14, 14-19 (Jun. 2000) (investigating the potential of ‘hacktivism’ as a tool in civil disobedience and fights against political injustice).
citizens who feel the need to contribute to their military’s or intelligence services’ real or imagined actions against an adversary state / organization by joining in an unofficial or vigilante capacity?

The unintended consequences of their actions may be horribly unhelpful and counter-productive or, potentially, may be beneficial. In either case, they would fall outside of protective legal frameworks and yet contribute to escalation potentially directed at different targets once attribution is achieved (or is assumed to have been achieved) by the original target.

III. ELECTRONIC SELF-DEFENSE

Whilst it appears self-evident that those of our citizens who may feel inspired to become part of a cyber-attack on assumed or known state adversaries will be outside of the employ of the state, it is extremely well-known that in other states, no such distinctions are held. Indeed, the blurring of the private and state-sector in terms of capability may be very significant. If it is assumed that capability is being made ready, trialed or even executed from non-military, non-state locations in adversary states – at what point is it legal to mount aggressive reconnaissance on those locations, pre-position electronic munitions to form a counter-strike, attempt to recruit or gain intelligence on the individuals who work there, and so on? At what point is pre-emptive, self-defensive attack legally legitimate?11

How is any legal position on these matters complicated or compromised by the dispersion of, for example, a somewhat or sometimes hostile state-owned, controlled or sympathetic business overseas – in the sovereign jurisdictions of our allies or even in our own state? What damage might we (accidentally) face inflicting on ourselves by targeting businesses that operate at the behest of a foreign power but that at the same time provide us or our allies with critical national infrastructure? Are we and our allies conscious of this dependence – even if it is of a second- or third-order? If we target business ‘x’ in a southeast Asian state, might a response come back through business ‘y’, which is not electronically connected with the original target but – being controlled by the host state – is utilized to apply a counter-measure (e.g. withdrawal of a critical national infrastructure service, explained as due to force majeure – thus nullifying any contractual leverage)?

Where does the law stand on all of these issues? Indeed, does the legal categorization even matter?

IV. THE SIGNAL POWER OF LAW AND ITS LIMITATIONS

Signaling has something to offer in terms of broadcasting clear consequences from a sound legal basis to all potential adversaries – and especially those deliberately identifying or considering identifying vulnerabilities in clearly non-military, non-state-owned infrastructure. Adversaries should have much to fear from either aggressive reconnaissance for targeting; probing for vulnerabilities; the brigading of focused capability; or the pre-placement of cyber-munitions or human assets. These and other activities need to be deterred. It may be that model of how the law could allow for hackback, and how parameters might be set for legally permissible retaliatory or defensive hackbacks).
existing domestic laws and, for example, the Laws of
Armed Conflict (LOAC) currently provide adequate legal
cover or could be adjusted to do so. However, even if this is
the case, the situation may not be clearly “signaled.” Even
if it were to be so signaled, the challenges of e-attribution
and the self-organizing swarm are massive. The deterrence
value (in the form of punitive sanctions) of law is of no
significance when cyber-warfare is so difficult to attribute
and where irritating swarms may self-assemble who, even
when employing low-tech scripting and hacking, may cause
problems by sheer volume of effort.

An issue to be raised is, then, what form of legally-
enabled signaling could dissuade swarming cyber-threats
who organize themselves into campaigning structures and
potentially have the guiding hand of a hostile power behind
them? In the era of unrestricted, unrestrained cyber-
warfare (where activists, mercenaries, proxies, criminals,
the misguided and others throw their hats into the ring) –
what are the cyber-penalties? Is a member of an assembled
swarm that causes loss of critical services (e.g. an
infrastructure attack resulting in power failure that leads to
patients dying in hospitals) culpable for a charge of
homicide? Given the low likelihood of most of these
culprits being physically apprehended – how (given limited
investigative resources) can adequate attribution be
achieved and what would comprise a cyber- or e-sanction,
or an e-penalty? What would be the gradated scale? How
can semi-permanent e-sanctions or e-penalties be enforced?

Given the backdrop of the hysterical and usually
unbalanced criticism of and lack of trust in national
technical authorities and others that has arisen as a result of

12 See JAMES A. LEWIS, ASSESSING THE RISKS OF CYBER TERRORISM,
CYBER WAR AND OTHER CYBER THREATS (2002), available at
reassessment of the threat of cyber war and its potential targets).
Snowden’s ‘disclosures’ – what will domestic, allied and international opinion on the pursuit of the ideas detailed above be? What freedom of maneuver remains? What forces or events could constrain or expand this maneuver space?

V. CONCLUSION

This thinkpiece paper has sought to problematize any lingering assumptions that legal remedies can flex and stretch to accommodate the threat environment in which our security and military apparatuses operate. However, there may well be some little deterrent value in signaling to would-be adversaries that – thanks to appropriate legal groundings – clear and punitive consequences will flow from any pre-emptive aggressive reconnaissance, let alone actual cyber-warfare attacks. More pragmatically, and somewhat beyond the scope of this paper, crisper signals may well be delivered by having the legally-provided ability to demonstrate to an adversary / mercenary / proxy that one already has the means to deliver punitive sanctions in acutely sensitive areas of their systems.

Given the deregulation of violence (cyber- and otherwise), the reduced barriers to entry for some cyberwarfare activities, and the ease with which swarms can be generated or may form spontaneously, legal deterrence or redress may only have any effect on those regimes who can be encouraged to comply with good behavior through diplomatic and other nonmilitary channels.
Legal Considerations on Cyber-Weapons and Their Definition

By Stefano Mele¹

Abstract:

The rapid evolution of scenarios and threats related to the increased use of cyber-space within the national security context, as well as an exponential spread of new and hypothetical “cyber-weapons,” as described at times with sensationalist language by the media, warranted a specific analysis of the phenomenon. The article focuses on the legal aspects of the “cyber-weapons” and gives for the first time a specific legal definition of cyber-weapons. Further analysis is dedicated to analyzing the most important malwares which defined and shaped the cybe-

This paper is based on “Cyber-weapons: legal and strategic aspects (version 2.0)”, which was published in June 2013 by the Italian Institute of Strategic Studies ‘Niccolò Machiavelli’ and is available at: http://www.strategicstudies.it/wp-content/uploads/2013/07/Machiavelli-Editions-Cyber-Weapons-Legal-and-Strategic-Aspects-V2.0.pdf.

¹ Stefano Mele is ‘Of Counsel’ to the Italian Carnelutti Law Firm, where his practice focuses on Technology, Privacy and Information Management Law. He holds a PhD from the University of Foggia. He is also Research Director on “Cyber-security & Cyber-Intelligence” of the Italian Military Centre for Strategic Studies (Ce.Mi.S.S.) of the Italian Ministry of Defense, and Director of the “InfoWarfare and Emerging Technologies” Observatory of the Italian Institute of Strategic Studies ‘Niccolò Machiavelli’. He is a lecturer for several universities and military research institutions of the Italian MoD and NATO, and has authored academic papers and articles on cyber-security, cyber-intelligence, cyber-terrorism and cyber-warfare topics.
security sector in the last two years, assigning them a specific legal classification in accordance with the newly-proposed definition of the term.

I. INTRODUCTION

Since September 2010, when former US Deputy Secretary of Defense William J. Lynn III publicly defined cyber-space as “the fifth domain of warfare”\(^2\) after ground, sea, air and space, the need to have practical rules regulating all aspects of cyber-warfare activities – especially from the point of view of international law – has become a priority for all international actors. The complexity of the subject makes this task particularly challenging. This is due to the existence of significant uncertainties and doubts over crucial and essential elements, for instance: the attacker’s anonymity and traceability; the so-called “preparation of the battlefield” for cyber-operations; the description of when a cyber-attack can be defined as an “armed attack”; the proportionality of the answer compared to the attack; the rules of engagement for cyber-space; and so on. Nonetheless, the scientific community is in the process of elaborating its findings, and reference to these findings can be found in a number of

commendable legal documents.\(^3\)

However, what is still missing in this debate is a legal consideration defining the term “cyber-weapon” and when a generic software or malware can be defined as such a weapon.\(^4\) It is crucial to define it for a correct evaluation of both the threat level from a cyber-attack, and the possible political and legal responsibilities, especially considering the costs that those governments\(^5\) and companies\(^6\) have to bear for each breach of the security of


\(^4\) Even the Black’s Law Dictionary has no definition for “cyber,” cyber-attack, cyber-warfare or obviously for cyber-weapon.


their computer systems.

In brief, weapons are tools through which, in a specific context, a subject can cause damage to another subject or object, or defend itself from an attack. Almost every State over time has enacted specific legislation to regulate the use of weapons, both for their classification and for their circulation. But what it is essential to highlight is that current international regulations actually do not clearly define the meaning of “cyber-weapon.” They only define the generic concept of a “weapon.”

From the point of view of military doctrine, even The Dictionary of Military and Associated Terms of the US Department of Defense (480 pages of definitions relevant to the defense sector) does not mention a generic concept of weapon, apart from mentioning non-lethal weapons (“a weapon that is explicitly designed and primarily employed so as to incapacitate personnel or materiel, while minimizing fatalities, permanent injury to personnel, and undesired damage to property and the environment”) and directly defining every specific type of weapon (or weapon system) except for cyber-weapons.

http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf; UK CABINET OFFICE ET AL., KEEPING THE UK SAFE IN CYBER SPACE (2013) https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace (British Government pointed out that 93% of large companies and 76% of small companies reported a cyber-attack in 2012, with a total cost for every single break-in calculated between £.110.000 and £.250.000 for the former ones and between £.15.000 and £.30.000 for the latter ones).


II. TOWARDS A LEGAL DEFINITION OF CYBER-WEAPON

To reach a precise definition of the concept of a cyber-weapon in the specific context of conflicts (warfare), it is necessary to separate it from the notion of malware typically used for cyber-crime purposes.\(^9\) It is easy to imagine how this complicates things since, as it happens for traditional weapons, cyber-warfare activities can be performed through malware and/or information technology tools which are also used to commit mere cyber-crime actions and that do not rise to the level of acts of warfare.

A further distinction has to be made also to differentiate cyber-weapons from malware and/or information technology tools used to perform espionage activities. Espionage represents the best and the most effective way to obtain – both in war and peacetime – political, military and economic advantages on both enemies and allies. This is also valid in the case of cyber-espionage.

Indeed, over the last decade, the digitalization and centralization of information (including classified information) and the lack of cyber-security awareness and education has made it possible for espionage to become one of the most critical threats to national security and to the competitiveness of each country. Nevertheless, historically, espionage has never represented the trigger of any known inter-state conflict. As espionage activities – nowadays strongly supported by technology – are carried out by every

\(^9\)See James P. Farwell & Rafal Rohozinski, The new reality of Cyber War, 54, 4 SURVIVAL: GLOBAL POLITICS AND STRATEGY 107 (2012) (to point out this difference, a part of the doctrine focuses on terms like “weaponised computer code” or “malware employed as ‘use of the force’”).
state, they are frequently tolerated by other states or, if they are carried out through extended “aggressive” strategies,\textsuperscript{10} in the worst case they might provoke only a reaction through specific economic sanctions.\textsuperscript{11}

Therefore, separating cyber-crime and cyber-espionage tools from the concept of cyber-weapons is a crucial element in this definition, especially because the use of a cyber-weapon could lead to the beginning of a conflict.

Having outlined the context for these considerations, it should be noted that, from an ontological point of view, a weapon can be also an abstract concept, thereby not necessarily a material one, as international and domestic legislation have considered it up to now. For these reasons, even a set of computer instructions – such as a program, or a part of a code and so on – can be considered a weapon when used in certain contexts with the specific purpose of sabotaging or damaging well-defined subjects and/or objects, through the use of certain means/tools. The aforementioned set of computer instructions can render to these kinds of intangible items the characteristic of a weapon, in this case, a cyber-weapon.

For those reasons, to reach a definition of cyber-weapon, it is necessary to focus on three essential elements:

\textsuperscript{10} See \textsc{David Wise}, \textit{Tiger Trap: America’s Secret Spy War with China} (2011); Posting of Stefano Mele to Formiche blog, \url{http://www.formiche.net/2013/02/20/hard-power-spionaggio-cinese/} (Feb. 20, 2013).

\textsuperscript{11} See Posting of Zachary K. Goldman to Snapshots blog, \url{http://www.foreignaffairs.com/articles/139139/zachary-k-goldman/washinton-secret-weapon-against-chinese-hackers} (Apr. 8 2013) (a recent introduction to the theme of the possible reactions to cyber-espionage activities); Alina Selyukh & Doug Palmer, \textit{U.S. law to restrict government purchases of Chinese IT equipment}, \textsc{Reuters} (Mar. 27 2013) \url{http://www.reuters.com/article/2013/03/27/us-usa-cybersecurity-espionage-idUSBRE92Q18O20130327} (concerning recent US Government policy in this sector).
[1]. **CONTEXT**: it must be the typical context of an act of cyber-warfare. This concept may be defined as a conflict among actors, both National and non-National, characterized by the use of information systems,\(^\text{12}\) with the purpose of achieving, keeping or defending a condition of strategic, operative and/or tactical advantage.

[2]. **PURPOSE**: of causing, even indirectly, physical damage to objects or people; or of sabotaging and/or damaging in a direct way the information systems of a sensitive target of the attacked subject.

[3]. **MEAN/TOOL**: an attack performed through the use of information systems, including the Internet.

In light of the above, a cyber-weapon can be defined as:

“A part of equipment, a device, or any set of computer instructions, used in a conflict among actors both National and non-National, with the purpose of causing (directly or otherwise) physical damage to objects or people, or of sabotaging and/or damaging in a direct way the information systems of a sensitive target of the attacked subject.”

Moreover, if it is true that currently a highly sophisticated cyber-weapon is exclusively the product of National activities or rather the work of one or more highly specialized criminal organizations that act on behalf of a State, it is also true that in the near future, common criminality might have cyber-weapons at its disposal. As a result, this will involve a clear alteration of the “CONTEXT”

---

\(^\text{12}\) The concept of information systems refers to the interactions among people, processes, data and technology. In this sense, the term is used to refer not only to information and communication technologies (ICT), but also to the way people use and interact with such technology.
element, which at the moment is closely defined to acts of cyber-warfare (political level), linking it to the economic interests typical of criminal activities (social level).

III. THE CLASSIFICATION OF STUXNET AND THE FOLLOWING MALWARE

On the basis of the definition just provided, Stuxnet can be classified as a cyber-weapon, as it represents a set of computer instructions (in the form of an executable program/malware), used in a conflict – in this case covert – among specific national actors\(^\text{13}\) \((\text{CONTEXT})\), aimed at modifying in a direct way the functioning of an Iranian sensitive target \((\text{PURPOSE})\), damaging it through the exploitation of information systems \((\text{MEAN/TOOL})\).

Stuxnet can be also considered as a cyber-weapon created with the sole purpose of sabotaging and damaging the specific sensitive information system of the target. Furthermore, it maintains this quality today because of the objective difficulty of reconfiguring it ontologically as a ‘non-weapon’ with only non-damaging functions.

On the contrary, dual-use cyber-weapons can be defined as “a part of equipment, a device, or any set of computer instructions” characterized by a possible dual (non-damaging) use, with indirect or unmediated damaging side effects. There are several examples of programs created to manage and fortify a computer system’s security which, if required, can be also used for offensive purposes. However, in a case where such software are actually used for offense, having the “\(\text{PURPOSE}\)” and the “\(\text{MEAN/TOOL}\)” elements unchanged, the “\(\text{CONTEXT}\)” element will have to

\(^{13}\) DAVID E. SANGER, CONFRONT AND CONCEAL: OBAMA’S SECRET WARS AND SURPRISING USE OF AMERICAN POWER (Crown Publishers 2012).
outline the psychological layer of the intent in order to legally classify the attack correctly.

Moreover, it is interesting to highlight that, since the public disclosure of Stuxnet, many other malware programs have drawn the attention of the public, thanks to the analysis work of security companies specializing in this sector. Flame, DuQu, Mahdi, Gauss, Rocra, and


18 Posting of GReAT to Securelist Incidents Blog,
FinFisher are a few of the most popular malware programs, defined as “heirs” of Stuxnet by the generalist press.

Nevertheless, placing the previously mentioned malware programs into the framework of the three defining elements proposed (“CONTEXT,” “PURPOSE” and “MEAN/TOOL”), there are today no other malware – publicly known – which can be classified as cyber-weapons. In the above cases, even presuming that the “CONTEXT” for each of them is an act of cyber-warfare (which may not be correct), and even having the “MEAN/TOOL” element, the “PURPOSE” of these malware programs is not one “[...] of causing (directly or otherwise) physical damage to objects or people, or of sabotaging and/or damaging in a direct way the information systems of a sensitive target of the attacked subject.” The common element characterizing them is another: obtaining information to carry out cyber-espionage operations. And, as stated above, espionage and cyber-espionage are not warfare.

The only exception to this assessment could come


from the analysis of the malware known as Shamoon.\textsuperscript{20} This malware program made the headlines in August 2012 for successfully hitting – \textit{inter alia}\textsuperscript{21} – something like 30,000 computers of the Saudi Arabian oil company Saudi Aramco, corrupting Aramco’s files and deleting the Master Boot Record of the infected machines, which is the sector of the hard disk containing the sequence of commands/instructions needed to boot the operating system.

The main purpose of Shamoon was to render the targeted information systems useless. For this reason, despite being far from the sophistication and the highly specialized manpower which led to the creation of Stuxnet, Shamoon’s “\textsc{Purpose}” in its simplicity was of “[...] damaging in a direct way the information systems of a sensitive target of the attacked subject” and of making that possible through the use of information systems (“\textsc{Mean/Tool}”).

As for the verification of the “\textsc{Context}” element, the attack against Saudi Aramco was claimed by a hacktivist group called “Cutting Sword of Justice.”\textsuperscript{22} Therefore, considering the open source data available and

keeping in mind the typically ideological and propaganda aspect of hacktivist groups, currently it is not totally correct to include this attack in a cyber-warfare context. As previously stated, a cyber-warfare action can be defined as: a conflict among actors, both National and non-National, characterized by the use of information systems, with the purpose of achieving, keeping or defending a condition of strategic, operative and/or tactical advantage.

However, if in the future the Shamoon attack was to be defined in a different context, for instance if proof emerged that the attack was sponsored by a state, it could be classified as a cyber-weapon.

Hence, as explained above, it is possible to outline further the typical elements of a cyber-weapon:

- its aim must be specific, therefore, the “part of equipment, a device, or any set of computer instructions” does not have to be created with the aim of reaching maximum diffusion, as generic malware is frequently designed (except for the case of concealment of the real purposes of an attack);
- the information systems which were hit must be classified as sensitive targets of the attacked subject;
- the purpose must be to actively penetrate the target’s information systems (not just to cause a simple dysfunction) with malicious ends;
- the information systems of the target must be protected; and
- tangible or significantly detectable damage must be caused.

Relying on the above claims, it is important to underline that the technical sophistication of cyber-weapons, the target-specific attention required, as well as

---

their high damage potential, requires a remarkable infusion of funds, time, and highly specialized manpower, as well as considerable intelligence information for their creation.

The need to rationalize these four elements leads one to believe that at this time a combination of efforts among one or more states and/or groups of cyber-criminals is necessary to create a cyber-weapon. The first is necessary for the economic backing and research financing, to collect intelligence on the target and the possible insertion/placement of the cyber-weapon in case of systems which are not directly connected to the Internet (as happened with Stuxnet) or easily accessible, while the second is useful to optimize time resources and for the employment of a specialized workforce.

As further proof, it is not a coincidence that the creation of Stuxnet seems to have been attributed to several non-governmental subjects, each of which was assigned to develop only a “piece” of the malware, without being aware of the range of the overall project.24

IV. ANTICIPATORY OUTLINES

Based on the discussion so far, cyber-crimes – above all those aimed at cyber-espionage,25 theft of

confidential information,26 and theft of intellectual property – are and will be, at least in the short-term, the main threat27 for information systems of both States and private companies, especially those which work in cooperation with governments. It is no coincidence that the so-called “heirs” of Stuxnet were designed exclusively to spread and infect their targets with the sole purpose of collecting information, or at most, of carrying out activities that can be classified as cyber-espionage (aimed at collecting intelligence information about potential targets of a future cyber-weapon).

If that is true, the two countries which are most likely to be the main protagonists of cyber-espionage and information theft – Russia and China – will keep on being the undisputed protagonists, also due to the collusion among leading politicians,28 intelligence services,29 and

26 The latest operation which hit the headlines was called “Luckycat”. Released by the security company TREND MICRO, this operation was addressed to 233 computers during 90 attacks which had as target several authorities and “sensitive” companies in Japan, India and Tibet. A report on the topic entitled “Luckycat Redux. Inside an APT Campaign with Multiple Targets in India and Japan” is available at http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_luckycat_redud.pdf. Also, the graphical data about exfiltration’s main operations of sensitive and reserved data which are currently known can be helpful. It can be found at http://blog.trendmicro.com/global-targets-infographic/.


28 See Klimberg, supra note 24.
groups of cyber-criminals\textsuperscript{30} or hacker patriots.\textsuperscript{31}

As things stand now, it could be argued that both Russia and China are and probably will increasingly be the two most active states in the field of cyber-warfare.\textsuperscript{32} Together with the United States and Israel, they will carry out a leading role in the conception, development, creation and employment of the next generations of cyber-weapons, or rather of software able to “self-learn” in real time how to sabotage or damage a target system directly from the analysis of the target system – and consequently to attack it autonomously.\textsuperscript{33}

\textsuperscript{29} It will suffice to consider that in 2006 more than 78\% of the 1,016 Russian political leaders were previously working for organizations affiliated to KGB and to FSB. For further research, see Interview by Evgenia Albats with Olga Kryshtanovskaya on Echo of Moscow, Feb. 4, 2007.


\textsuperscript{31} People who have high technical capacities and are politically motivated to act for and in the interest of their country.


\textsuperscript{33} THOMAS RID, CYBER WAR WILL NOT TAKE PLACE 54 (Hurst & Co. Publishers 2013).
Finally, a medium-term analysis shows that Iran will play a role very similar to the ones currently carried out by Russia and China, and, though to a lesser extent, North Korea. Both countries show an increased interest in these fields and are increasing their investments in economic and human resources to this end.


V. CONCLUSIONS

The protection of national strategic assets, which nowadays can be compromised by a cyber-attack, almost instantly is and must always be the priority, whether we are facing cyber-warfare activities or actions aimed exclusively at seizing the sensitive and/or classified information of governments.

A correct understanding of the concept of cyber-weapon – including a legal definition – is the main and urgent objective that must be achieved. This will allow the evaluation of both the threat level coming from cyber-attacks, and the direct political and legal responsibilities of the authors of the attack.

Furthermore, only with the appropriate attention on legal definitions and the creation of a commonly accepted set of rules, will it be possible to start addressing these issues which urgently require a very pragmatic response. The urgency is apparent, especially now that, due to the lack of valid technical (traceability of attacks) and judicial (responsibility for the attacks) answers, the majority of the governments are trying to speed up the innovative and takeover processes of cyber-weapons, in order to easily steal confidential information, but also to possibly sabotage or damage the enemy’s military networks.36

The challenges that governments, the Armed Forces and National Security Institutions are, and will be, facing increasingly in the field of cyber-security and cyber-intelligence are certainly as complex as they are fascinating. Cyber-weapons require an adaptive response

approach, which includes both the technical-technological research sector and the strategic, operational and tactical sectors. For the first time, the latter sectors are experiencing their exposure and vulnerability to vanishing of their typical sectorial partition right through to the Internet and technologies.

Defining with certainty what constitutes a cyber-weapon, and when a cyber-attack on sensitive targets can be considered as a ‘use of force’, or an ‘armed attack’ represents a common priority by now, especially in the modern Western world which is interconnected and bases its entire social welfare on the functioning of information technologies. The US Government began paving the path, but an increasing number of countries have started to modify their strategies even providing for offensive military operations via cyberspace. The future of cyber-attacks will be a challenging one.

Internet Communication Blackout: 
Attack Under Non-International Armed Conflict?

By Cassondra Mix

Abstract:

The internet has become both a significant tool and vulnerability in most States’ national security stratagem. Control of the internet could easily become a real part of modern armed conflict in the upcoming years. This was exemplified by Egypt’s decision to cut off internet access within its borders during its January 2011 uprising. This paper will use the experience in Egypt as a case study, and argue that even if the violence of the protests had risen to the level of armed conflict, it is unlikely the governmental actions taken by Egypt would be classified as an attack under the law of armed conflict.

I. INTRODUCTION

In January 2011, the people of Egypt took to the streets seeking social reform. On January 25th, protests began. The countrywide protest was organized primarily through the use of social media sites like Facebook and

1 The Author is a recent graduate from J. Reuben Clark Law School - Brigham Young University. The Author would like to thank her parents for their love and support, and Professor Eric Jensen for all his help, guidance, and encouragement.

Twitter. The “Day of Rage,” as it is known, began as a peaceful gathering of citizens across the country of Egypt, but soon became violent. The first deaths on both sides occurred on that day, and the death count continued to rise the following day.

Due to the wide usage of social media sites for organizational and communicational purposes the government of Egypt made the decision to shut down access to these sites on January 27th. The next day, the government limited public internet access. The same day troops were ordered into the streets, but they did not interact with the protestors or police. The announcement that President Mubarak was dismissing top officials in the government had no effect on the protestors.

The internet was partially restored on February 2nd after 5 days of the government imposed blackout. The protests continued. After 18 days of protests, on February 11th, President Mubarak resigned and governmental control of Egypt was turned over to the army. At the end of the protests the final death count numbered in the hundreds.

It seems clear that the use of social media significantly facilitated not only the organization of the

---

4 Id.
5 Id.
6 Id.
7 Id.
8 Id.
9 Id.
10 Id.
11 Id.
12 Id.
13 Id.
protest but also shaped the way the events were shared with the world. Social media sites allow for almost instantaneous free interchange of ideas and information. This is only one of the reasons that these sites are used to organize movements all over the world. One activist in Cairo was quoted as saying, “We use Facebook to schedule the protests, Twitter to coordinate, and YouTube to tell the world.”

Internet use is becoming increasingly integrated into all that we do. “From 2000 to 2010, global internet usage increased from 360 million to over 2 billion people.” People use the internet to communicate with each other through such things as VoIP, emails, and video conferencing. Even the very nature of how people fight wars has become dependent on the use of the internet. The internet allows almost instant communication, facilitating movement of troops and coordination of operations around the world. It also increases the vulnerabilities of critical infrastructure, such as water treatment plants and power grids.

Attempts have been made and are being made to apply the law of armed conflict to cyber warfare. In

14 See Bhuiyan, supra note 2, at 16.
16 Id.
some instances this has been successful; in other instances application has just created more questions. For example, one can successfully apply the principle of distinction, prohibiting “attacks that cannot reasonably be limited to a specific military objective and which are indiscriminate or haphazard in their inclusion of civilian targets,” to the cyber world. This is relatively straightforward. Attacks must be specifically targeted at military objectives and limit the collateral damage on civilian targets. However, application of this principle creates confusion when determining the level of collateral damage assessment required before an attack is made in cyberspace to keep the operation in compliance with the law of armed conflict. Much progress needs to be made in this area of law.

This transition into the digital age raises many questions about how we use the internet. The legalities of internet use not only affect how we can use the internet as individuals but also have implications for states. The events of the January 2011 uprising in Egypt raise questions about the legalities of state use and regulation of the internet. The use of the internet has become a tool in most militaries’ arsenals. Attempts to block the internet could easily become a real part of modern warfare in the

http://www.ccdcoe.org/publications/virtualbattlefield/07_HUGHES%20Cyber%20Regime.pdf (discussing the need for a global application of the Law of Armed Conflict to cyber warfare); Jeff Schogol, Official: No options ‘off the table’ for U.S. response to cyber attacks, STARS AND STRIPES (May 8, 2009), http://www.stripes.com/article.asp?section=104&article=62555 (Air Force Gen. Kevin P. Chilton has said that "[t]he Law of Armed Conflict will apply to this domain.").


20 Id. at 3.
upcoming years. Understanding the legalities of operations like this one will be vital to functioning within the law of armed conflict.

This concern over the internet and its connection to armed conflict is illustrated by the experience in Egypt described above. President Mubarak impacted internet connectivity within Egypt to preserve national security in the face of potential armed conflict. While armed conflict never erupted in Egypt, it certainly could have as it did in other states involved in the Arab Spring. Therefore, it is worth considering how President Mubarak’s blackout of the internet would have been viewed if the laws applicable during a non-international armed conflict would have applied. More specifically, would such actions have been classified as an “attack” in this hypothetical situation? To answer this question, this paper will use Egypt as a case study by building off the facts of the January 2011 uprising and assume that before Egypt made the decision to limit internet access the violence of the protests had risen to the level of armed conflict.21

In a situation like the proposed hypothetical, severing the internet within the borders of a country during a non-international armed conflict would not be considered an attack under *jus in bello* or law of armed conflict. This paper will address the legal reasoning behind this conclusion. Section II will discuss the type of law that is to be applied to the situation. Section III defines an “attack” under applicable laws and presents a proper methodology

---

21 See *generally* Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 2-3, Aug. 12, 1949, available at http://www.icrc.org/ihl.nsf/WebList?ReadForm&id=365&c=com (articles 2 and 3, which discuss what triggers application (armed conflict), are common to all the Geneva Conventions and so the commentary for these articles is the same for all the conventions).
for applying this definition in cyber warfare. Section IV will apply that methodology to the hypothetical armed conflict in Egypt and explain why the actions taken by Mubarak’s government would not be considered an attack.

II. LEGAL PARADIGM: TYPE OF LAW

The type of law that is applied in any armed conflict depends on the classification of the conflict. Current bifurcation of the law of war into international armed conflict (IAC) and non-international armed conflict (NIAC) was set forth in the Geneva Conventions of 1949.\textsuperscript{22} The classification of a conflict is extremely important in discerning the applicable law. The full body of the law of armed conflict is applicable in an international armed conflict while only select parts, such as Common Article 3 of the Geneva Conventions, are applicable in a non-international armed conflict.

Prior to 1949, there was no bifurcation of the law of armed conflict.\textsuperscript{23} The law at that time was designed to only apply to international conflicts.\textsuperscript{24} International conflicts then were basically war between two states. Internal conflicts, more commonly known as civil wars, were not subject to any international regulation.\textsuperscript{25} Until 1949, states refused to draft any such regulations because they felt that “insurrection and rebellion were a purely domestic matter”


\textsuperscript{23} ROBERT KOLB & RICHARD HYDE, \textit{AN INTRODUCTION TO THE INTERNATIONAL LAW OF ARMED CONFLICTS} 65 (2008).

\textsuperscript{24} \textit{Id}.

\textsuperscript{25} \textit{Id}.
that should have no external regulations.\footnote{Id.}

In the wake of the Spanish Civil War and World War II, it was clear that there was a “stark absence of protections for civilians in wartime.”\footnote{Gary D. Solis, The Law of Armed Conflict: International Humanitarian Law in War 97 (2010).} While most states did not want to give up any sovereignty, they realized after these wars that there was a need for some minimal protections for civilians during internal conflicts.\footnote{Crawford, supra note 22, at 8.} Common Article 3 of the 1949 Geneva Conventions was the solution.\footnote{Crawford, supra note 22, at 8.} It laid out the fundamental principles that must guide all non-international armed conflicts.\footnote{Id. at 9.}

In a nutshell, common Article 3 requires humane treatment of persons not taking direct part in hostilities and those placed \textit{hors de combat},\footnote{Solis, supra note 27, at 98.} “[doing] little to regulate combat or protect civilians against the effects of hostilities.”\footnote{James G. Stewart, Towards a single definition of armed conflict in international humanitarian law: A critique of internationalized armed conflict, 85, 850 IRRC 313, 320 (2003), available at http://www.icrc.org/eng/assets/files/other/irrc_850_stewart.pdf.} It only applies to hostilities that reach the level of armed conflict.\footnote{Id. at 318.} It is important to note that originally when common Article 3 applied no other part of the Conventions applied.\footnote{Solis, supra note 27, at 99.} This means that provisions like Prisoner of War protections do not apply to a non-international armed conflict because they are contained in areas other than common Article 3.\footnote{Id.} Common article 3 is now considered to apply to all armed conflicts as a matter

Over the decades following the Geneva Conventions of 1949, the nature of armed conflicts continued to undergo significant changes.\footnote{Crawford, supra note 22.} The frequency and intensity of armed conflicts increased, most of these being of a non-international character.\footnote{Solis, supra note 27, at 99.} Most casualties during non-international armed conflicts were consistently civilians.\footnote{Crawford, supra note 22.} States were beginning to realize that “[t]he de minimus rules provided for in Common Article 3 were insufficient to the task of regulating such widespread and brutal conflict.”\footnote{Id. at 11.} Modification of the current law was needed.\footnote{Solis, supra note 27 at 120.}

applied in a non-international armed conflict.\textsuperscript{44} For example, APII only applies to a subset of non-international armed conflicts. Instead of applying to “armed conflicts not of an international character,” APII limits its application to:

“[A]ll armed conflicts which are not covered by Article 1 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) and which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol.”\textsuperscript{45}

This means that, in contrast to common Article 3, APII does not apply to situations like the warring of two dissident groups.\textsuperscript{46} The requirement of exercising control over part of the territory also excludes the “activities of the Irish Republican Army in Ireland, the Basque Separatists in Spain, and the Shining Path in Peru.”\textsuperscript{47} The ICRC has pointed out that the criteria set forth in APII makes it impossible to apply APII in all cases of non-international armed conflict.\textsuperscript{48}

Throughout this period of change, situations arose

\textsuperscript{44} Crawford, \textit{supra} note 22, at 16.
\textsuperscript{45} APII, \textit{supra} note 43.
\textsuperscript{46} Stewart, \textit{supra} note 32, at 319.
\textsuperscript{47} Solis, \textit{supra} note 27, at 131.
\textsuperscript{48} Solis, \textit{supra} note 27, at 131.
that didn’t fit neatly into the bifurcated system. One example would be internationalized armed conflicts. “Internationalized” armed conflicts are conflicts that do not rise to the level of an international conflict but transcend the category of non-international conflict.\(^{49}\) An illustration of this type of conflict would be situations that began as a non-international armed conflict but because of third state intervention fall out of this classification.\(^{50}\) This mixed conflict category began to blur the lines between international armed conflict and non-international armed conflict.\(^{51}\)

The armed conflict in Lebanon provides a historic example of a mixed conflict category.\(^{52}\) Since 1975, Lebanon has suffered from armed conflict between warring groups within its borders.\(^{53}\) In March of 1978, Israeli forces intervened in the southern part of Lebanon followed by a period of occupation.\(^{54}\) This action by Israel moved Lebanon’s conflict into something more than a non-international armed conflict but less than an international armed conflict (because Israel was not fighting against the Lebanese government).

This blurring is highlighted in the development of customary law. The United Nations General Assembly Resolution 2444, dated 19 December 1986, notes “the necessity of applying basic humanitarian principles in all

\(^{49}\) Crawford *supra* note 22, at 16.

\(^{50}\) *Id.*

\(^{51}\) *Id.* at 18.


\(^{53}\) *Id.*

\(^{54}\) *Id.* at 157.
armed conflicts.” Even though the UN resolution itself is non-binding, that same year the International Court of Justice (ICJ) recognized that certain elements of the law of armed conflict are applicable regardless of the type of armed conflict. Specifically, it noted that the principles in Common Article 3 are applicable in “the event of international armed conflicts, . . . in addition to the more elaborate rules which are also to apply to international conflicts; and they are rules which, in the Court's opinion, reflect what the Court in 1949 called ‘elementary considerations of humanity’.”

In 1995, the International Criminal Tribunal of Yugoslavia (ICTY) recognized this major change, writing, “the aforementioned distinction [between international armed conflict and non-international armed conflict] has gradually become more and more blurred, and international legal rules have increasingly emerged or have been agreed upon to regulate internal armed conflict.” In its view, the need to protect civilians shouldn’t differ between conflict types.

“Why protect civilians from belligerent violence, or ban rape, torture or the wanton destruction of hospitals, churches, museums or private property, as well as proscribe weapons causing unnecessary suffering when two sovereign States are engaged in war, and yet refrain from

56 Military and Paramilitary Activities, supra note 36.
57 Id.
enacting the same bans or providing the same protection when armed violence has erupted ‘only’ within the territory of a sovereign State?“59

While the application of international armed conflict principles to non-international armed conflict situations was a big step towards eliminating the separation between the two, it does not equate to equal coverage. The ICTY clarified the application of these rules was limited to only a certain “number of rules and principles.”60 Additionally, it stated it is the “general essence of those rules, and not the detailed regulation they may contain” that pertain to non-international armed conflicts.61

State practice also reflects this movement of using international armed conflict principles in non-international armed conflict situations.62 A recent study by the International Committee of the Red Cross (ICRC) of customary laws in international armed conflict and non-international armed conflict found that many areas of law in international armed conflict have crossed over into non-international armed conflict situations.63 There have been many criticisms of the study. One critique involves the extensive use of military manuals as evidence of state

59 Id.
60 Id. at ¶ 126.
61 Id.
62 Crawford, supra note 22, at 26.
63 Jean-Marie Henckaerts, Study on customary international humanitarian law: A contribution to the understanding and respect for the rule of law in armed conflict, 87, 857 IRRC 175, 198 (Mar. 2005), available at http://www.icrc.org/eng/assets/files/other/irrc_857_henckaerts.pdf (there have been many criticisms of the study but the overall trend in state practice of the application of IAC principles in NIAC situations still holds true).
practice.64 Military manuals are a combination of law and policy.65 In addition, the manuals do not always reflect actual implementation.66 Another area that has received censure is the inconsistent application of the term “virtually uniform”67 in deciding if state practice is customary law.68 While there have been many criticisms, the results of the study continue to provide informative assistance into the migration of international armed conflict principles to non-international armed conflict.69

One example of how principles of international armed conflict have migrated to non-international armed conflict is use of a flag of truce. This rule comes from the Hague Convention of 1907 article 32.70 A fighter bearing a white flag of truce is immune from attack as long as he does not take part in hostilities.71 While originally only applicable in international armed conflict, through extensive state practice, it has come to be considered customary law and applicable in non-international armed

---

65 Id.
66 Id.
67 See William H. Boothby, Weapons and the Law of Armed Conflict 37 (2009) (state practice has to be virtually uniform, extensive and representative to establish a rule of customary international law).
68 Id.
69 Crawford, supra note 22, at 32.
71 Id.
conflict situations as well.\textsuperscript{72}

Understanding the migration of international armed conflict principles into non-international armed conflict situations is vital to applying appropriate laws. Knowing what portions of targeting law and detention law have now migrated into non-international armed conflict allows states to more fully apply the law. However, confusion remains in many cases and allows states to manipulate the applicability of the law to suit their needs. An illustrative example of this situation is the United States’ War on Terror.

After the attacks of 9/11 the United States declared a War on Terror.\textsuperscript{73} This War on Terror is unlike any war before. It involves a state fighting against a non-state actor on an international scale. Such a conflict does not fit neatly into any specific classification. Without a specific classification, it is difficult to determine the applicable laws in situations like the treatment of detainees. In a memorandum issued by Pres. George W. Bush in 2002, the U.S. determined that “none of the provisions of Geneva apply to [the] conflict with al Qaeda in Afghanistan or elsewhere throughout the world because…al Qaeda is not a


High Contracting Party [to the Convention].” This meant for the U.S. that the War on Terror was not an international armed conflict as defined by the Geneva Conventions. As a result, none of the provisions on the treatment of prisoners of war applied to the War on Terror.

In this same memorandum it was also argued that the War on Terror was not non-international armed conflict under common Article 3 because “the relevant conflicts are international in scope and common Article 3 applies only to ‘armed conflict not of an international character’.” Therefore, the War on Terror was deemed to fall outside of the bifurcated classifications of the law of armed conflict and as a consequence none of the laws applied. Although the U.S. Supreme Court later declared that common Article 3 applied to the War on Terror, there is still confusion about the required treatment of detainees under common Article 3. The U.S. used this confusion to justify controversial interrogation techniques that arguably crossed the line of humane treatment.

The confusion concerning the applicable laws of armed conflicts in all varieties of conflict needs to be

74 Memorandum from George W. Bush on Humane Treatment of al Qaeda and Taliban Detainees to The Vice President et al., 1 (February 7, 2002), available at http://www.aclu.org/files/assets/20100615_dos_release_1_doc_already_released.pdf.
75 Id. at 2.
78 Id. at 5.
eliminated. It is important for states to understand what law governs different levels of conflict so that they will not mistakenly violate the appropriate rules. In addition, states must be able to characterize operations under the correct context so as to correctly apply the law to their actions. The next section will help to clarify what laws apply to cyber warfare in non-international armed conflicts and lay out a framework for states to use.

III. “CYBER ATTACK”

The prior discussion of the applicability of International Armed Conflict rules to Non-International Armed Conflicts is important for this paper because the legality of Egypt’s actions in shutting down the internet during the hypothetical armed conflict is dependent on the characterization of that action as an “attack,” as that term is borrowed from the principles of International Armed Conflict. It is important to understand that if an action taken during an armed conflict would fall into the “attack” category, it will affect the legality of the action and place limits on the action itself. More specifically, if the actions taken by Egypt to shut down the internet amount to an attack, then Egypt’s actions during its armed conflict with the protestors are governed by additional principles that might limit, as a matter of law, the actions that Egypt can take. However, there is no definition of the word “attack” in common Article 3 that would provide a method for interpreting Egypt’s actions. Because of this lack of clarity, most scholars look to the definition of “attack” under international armed conflict.

This section will expand what an “attack” means in the context of cyber warfare beginning with what constitutes an attack in non-international armed conflict. Following that, it will determine what the core element of an attack is. Next, it will look at what test should be used
to classify something as an attack. Finally, some examples will be given of applying the chosen approach to cyber operations.

API defines “attacks” as “acts of violence against the adversary, whether in offence or defence.”\(^{79}\) Using the term “violence” seems significant when considering the scope of actions that would fit within the definition of attack. While this protocol is only applicable in international armed conflict situations, the ICRC commentary to APII records that the definitions in API were to apply to both protocols.

"" Definition of attack ' Protocol I defines attacks. This term has the same meaning in Protocol II. Article 49 ' (Definitions of attacks and scope of application), ' paragraph 1, of Protocol I, reads as follows "Attacks" means acts of violence against the adversary, whether in offence or defence."\(^{80}\)

Attack is also defined in The Manual on the Law of Non International Armed Conflict (NIAC Manual). The NIAC Manual was written by three prominent LOAC scholars who were writing under the auspices of the San Remo Institute and for the purpose of establishing what laws apply in a non-international armed conflict. In defining “attacks,” they followed the language of API. They noted in their commentary that this is where they derived their definition because the drafters of API and APII agreed that the two protocols would have the same

\(^{79}\) API, \textit{supra} note 42, at art. 49.

definition of attack.\(^{81}\)

Though the U.S. is not a Party to API, it has declared many parts to be customary law,\(^{82}\) and has not specifically objected to the definition of attack. Many of the articles use the word “attack”, and apply it as defined by API.\(^{83}\) In view of that, this definition of “attack” could be viewed as customary law. Accordingly, it is proper to use this definition in non-international armed conflicts.

With the migration of “attack” from international armed conflict to non-international armed conflict comes the migration of other principles, such as military objective, distinction and proportionality, associated with attacks. These additional principles migrate because they are linked to the application of attack and the law of non-international armed conflict does not have any corresponding principles.\(^{84}\) They are necessary for states to plan and carry out attacks during non-international armed conflicts. This is significant because it once again blurs the lines between the laws of international and non-international armed conflicts.\(^{85}\) APII part IV talks about targets that are protected from attack, however, it does not include any principles for use in targeting. Therefore, API articles 51, 52, and 57 must be used to define these principles.\(^{86}\)

The principle of distinction requires differentiating between civilian persons and objects and military persons

\(^{81}\) Schmitt et al., supra note 72, at § 1.1.6.
\(^{83}\) Id.
\(^{84}\) Kolb & Hyde, supra note 23, at 257.
\(^{85}\) Id. at 259; see also Henckaerts, supra note 63.
\(^{86}\) See Schmitt et al., supra note 72.
and objects when attacking the enemy.\textsuperscript{87} This principle is stated in API art 48.

\textit{“Article 48. BASIC RULE. In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.”}\textsuperscript{88}

It seeks to protect those civilians who are not directly participating in hostilities by protecting them from its effects.\textsuperscript{89}

The principle distinction is important in a non-international armed conflict because it prohibits governments from retaliating against the civilian population as a whole for the acts of one group. This principle makes it illegal for states to bomb a large portion of a city full of civilians because there are a handful of fighters located there. The government must target the fighters specifically and limit the damage to civilian life and property.

Military objects are “those objects which 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{90} Objects are limited to those that would \textit{effectively} make a military contribution. This would include weapons, bridges that are used by armed forces and buildings that hold

\textsuperscript{87} Id. at § 1.2.2.
\textsuperscript{88} API, \textit{supra} note 42, at art. 48.
\textsuperscript{89} SCHMITT ET AL., \textit{supra} note 72, at § 1.2.2.1.
\textsuperscript{90} API, \textit{supra} note 42, at art. 52.
military meetings and personnel. Using an example from the scenario, the server hosting the social media site used by the protestors for communication would be a military objective because it allows communication between protestors and its destruction offers a definite military advantage.

The rule of proportionality requires a party to “[r]efrain from deciding to launch any attack which may be 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.” This means that the damage and loss of civilian lives cannot be excessive when weighed against the value of the target.

In a non-international armed conflict, proportionality would mean that “[a]ll attacks must also be conducted bearing in mind the principle of proportionality.” The test would be to weigh the value of the military advantage of a target against “the expected harm to civilians and civilian objects.” If the harm is excessive in comparison then the attack would be forbidden. For instance, when deciding whether or not to attack a national power grid, the military benefit would be weighed against the possible damage that might result in loss of life or property. In this example it would be necessary to consider the effects on places such as hospitals that might not have sufficient backup generators to maintain operation during a power outage.

The migration of “attack” from international armed

91 SCHMITT ET AL., supra note 72, at § 1.1.4.3.
92 API, supra note 41 42, at art. 57(2)(a)(iii).
93 SCHMITT ET AL., supra note 72, at § 2.1.1.4.4.
94 Id. at § 2.1.1.4.5.
95 Id. at § 2.1.1.4.9.
96 Id.
conflict to non-international armed conflict produces large shifts in the law of armed conflict. The movement has blurred the lines between the two types of armed conflict. These lines will continue to blur as the nature of armed conflicts continues to change.

In looking at the elements of attack, the essence seems to be “acts of violence.” Violence is characterized as “intense...often destructive action or force.”97 Pulling an example from the kinetic world, an act of violence would be launching a rocket-propelled grenade. The result of pulling the trigger leads to a destructive and potentially deadly grenade explosion. Applying this definition to the cyber world requires a more subtle approach. Pushing a button (the action), which sends a virus like Stuxnet, could have violent results. The Stuxnet infiltration of Iranian computers caused actual damage to physical property.98 Nonetheless not all viruses cause physical damage. Some cyber operations are as simple as a Distributed Denial of Service (DDoS) which shuts down a website by overwhelming it with requests, but causes no physical damage.99

In deciding whether or not an action would be considered an attack, there must be some test to guide the classification. Paul Walker proposes that an effects or consequence test would be the most appropriate test to use for this determination.100 In reaching this conclusion, he

100 Walker, supra note 82, at 21.
discusses three methods: “actor-based,” “results-based” and “consequence-based.” Walker analyzes each method’s effectiveness in classifying cyber operations as attacks.

The first method discussed was the “actor-based” methodology.\textsuperscript{101} This test defines “any action occurring between two forces engaged in combat” as an attack.\textsuperscript{102} This rule is based on the Commentary of article 49 of API.\textsuperscript{103} Under this method, every action taken by a military force against another force would be considered an attack whether or not the action was violent in nature.\textsuperscript{104} For instance, infiltrating an enemy’s network system to gather data would be considered an attack. Even if the intrusion was not violent and no damage resulted, it was an action taken against an opposing force.

The over-inclusiveness of this test is a serious stumbling block. This test would count actions such as espionage and psychological operations as attacks.\textsuperscript{105} Most states would not accept this test because of the limitations it places on existing state practice.\textsuperscript{106} Examples of state practice that would be affected include the “long-held notions regarding the distinction between espionage and attacks, especially where computers and computer networks are involved.”\textsuperscript{107} Most states would not want to

\textsuperscript{101} Id. at 15.
\textsuperscript{102} Id. at 16.
\textsuperscript{103} Id. at 15.
\textsuperscript{104} Id. at 16.
\textsuperscript{105} Id.
\textsuperscript{106} Id. at 16; see also Paul Eckert & Phil Stewart, Chinese entities world's biggest economic spies: Pentagon, Reuters, May 19, 2012, available at http://www.reuters.com/article/2012/05/19/us-usa-china-military-idUSBRE84I06X20120519 (there have been many recent incidents between the U.S. and China about the use of economic cyber espionage in the past year, but neither the U.S. or China would consider this an attack).
\textsuperscript{107} Walker, supra note 82, at 16.
place this practice in jeopardy.\textsuperscript{108}

The “results-based” methodology looks at attacks from the opposite view. It asks if the operation accomplishes the same outcome that could have been reached with “bombs or bullets.”\textsuperscript{109} This test also doesn’t limit its application to operations with violent results.\textsuperscript{110} There is no room for distinction between kinetic and cyber actions. For example, a DDoS action that does not result in any physical damage but shuts down the computer system would be classified as an attack under this approach.\textsuperscript{111} The cyber result of shutting down the computer system would be the same if you used cyber or kinetic means.

This test also does not take into account the possibility that an action might have been achieved without using “bombs or bullets.”\textsuperscript{112} For instance, an air traffic control tower could be shut down due to the actions of an undercover agent just as effectively as using a bomb but without all the resulting property damage.\textsuperscript{113} Classifying attacks using this method would severely limit the aims of humanitarian laws by not allowing non-violent actions to be used in place of destructive methods.\textsuperscript{114}

The “consequence-based” method or effects test looks at the consequences of an action.\textsuperscript{115} If the effects of an action are violent then it is classified as an attack.\textsuperscript{116} The classification of the action is based on the potential violent consequences which must be reasonably

\textsuperscript{108} Id.
\textsuperscript{109} Id. at 17.
\textsuperscript{110} Id. at 18.
\textsuperscript{111} Id.
\textsuperscript{112} Id. at 20.
\textsuperscript{113} Id.
\textsuperscript{114} Id. at 19.
\textsuperscript{115} Id. at 20–21.
\textsuperscript{116} Id. at 20.
foreseeable.117 Reasonable foreseeability implies that “constant care” be taken in all military operations to spare the civilian population and objects.118 In cyber operations, for example, it would mean things such as keeping a current understanding of the targeted network in anticipation of potential overflow effects onto civilian objects from an operation.

It is also necessary to define what would be a violent consequence. Without a method for determining if a consequence is violent it cannot be determined if an act was an attack as understood under API. Walker defines violent consequences as those causing injury or death, physical damage or destruction.119 Mere inconvenience or deterioration in quality of life does not rise to the level of violence.120 This method seems to be the most widely-accepted test used by scholars in classifying cyber actions121 and will be the test used in this paper.

Taking a look at some examples of violent and non-violent consequences, it becomes easier to recognize the distinction. In India and Bangladesh, there has been an

118 API, *supra* note 42, at art. 57.
120 *Id.*
121 *See* Michael N. Schmitt, *Wired Warfare: Computer Network Attack and Jus in Bello*, 84, 846 IRRC 365 (2002), available at http://www.icrc.org/eng/assets/files/other/365_400_schmitt.pdf; Walker, *supra* note 82, at 16 (Many expert scholars have used the “effects-based” methodology, and it has been applied in both *jus ad bellum* and *jus in bello*).
exchange of cyber operations defacing various websites. Most forms of defacement involve replacing the main webpage of a site with some type of propaganda message or image. In the example of India and Bangladesh, Bangladeshi hackers have replaced the web content with “Bangladeshi flags and images of people tortured by Indian border guards.” Even though the websites and their content are usually unavailable for a period of time there is no resulting physical damage or destruction of property. The effects of this operation would not be considered violent consequences, thus, this would not be an attack.

In August 2012, Aramco – a state-owned oil company – was the target of a cyber-operation. The state attributed this act to unnamed “foreign countries.” It came in the form of a computer virus introduced to the company’s computer network through an e-mail. The virus was reported to have “destroyed data on servers and erased hard-drives on individual computers.” While

123 While many of these operations are undertaken by civilians, the principles are equally applicable to state and non-state actors.
125 Id.
127 Id.
128 Id.
129 Id.
there was no disruption of oil output, the destruction of data would be considered physical damage to property. This result would fall into the category of a violent consequence, making this operation an attack.

It is also important to note that the object used to attack does not have to be classified as a weapon. Pulling from an example in the kinetic world, during the Persian Gulf War, Iraqi soldiers were buried alive using a plow attached to the front of a tank. The act of burying the soldiers alive is an attack, but the instrument used to carry out this attack, the plow, is not considered a weapon. The same principle applies in the cyber world. The instrument used to carry out an operation may not be categorized as a weapon, but the action could still be an attack. Conversely, just because a tool is called a weapon does not mean that every time it is used that action is an attack. In the cyber world a malicious piece of software, which is classified as a cyber-weapon, could be used in an operation without that operation being considered an attack. For instance, a cyber-weapon could be used to map a network in anticipation of a future attack without executing any actual attack, despite its capacity for such an action.

The “consequence-based” (effects test) is the most appropriate test to use. This methodology of looking at the effects of an action to determine its classification is easy to apply, making it an effective test for commanders and legal

130 Id.
advisers to use. It does not have the over-inclusiveness problem of the “actor-based” methodology. It also gives the ability to distinguish between kinetic and cyber actions, which is not possible under the “results-based” method. Returning to the example of the Iranian Stuxnet virus, it’s now clear that that would qualify as an attack under the effects test because sending the virus resulted in physical damage to the property.  

Conversely, the DDoS action that shuts down a website would not be an attack because there was no physical damage to the property even though in the past this would have only been possible though the use of “bombs or bullets.”

IV. Application to Hypothetical

In applying this approach to the hypothetical, caution must be taken to remember that this is a jus in bello issue in a non-international armed conflict situation. In other words, in opposition to the actual facts of the uprising in Egypt where there was no armed conflict, the hypothetical assumes an existing armed conflict between the government of Egypt and various groups trying to overthrow that government. As discussed above, the law of armed conflict as applied to international armed conflicts has migrated over into non-international armed conflicts. Thus, the definition of attack from API applies in this situation. In this section, Walker’s effects test will be applied to the facts of the scenario. It will be shown that shutting down internet access is not an attack.

A. State Actors

As a reminder, here are the basic facts of this hypothetical. The citizens of Egypt rose up in protest of the government. This protest became a non-international armed conflict. In an attempt to combat the use of the internet in organizing the protests, the Egyptian government severed internet access. This was done by calling each of the four ISPs and telling them to shut down access to the internet.  

134 Each ISP pulled all Egyptian internet address from the global routing tables.  

135 The four ISPs disconnected Egypt from the internet non-simultaneously within a period of about 13 minutes.  

136 This blackout continued for 5 days.

When using the effects test to evaluate the government actions the first thing to look at is the results of the action. The effects are those which proximately result from the action on the ISP itself. Any reverberating effects must be “foreseeable in light of the information reasonably available to the attacker at the time.”  

137 Severing the internet resulted in a loss of business for the ISPs and internet based companies, and no internet access to the citizens of Egypt. No internet meant that the citizens had no email, VoIP, or social media access and the protestors had no means of communication.

Any financial harm to the owners of the ISPs or other businesses is not property damage or destruction. At most it would be considered a deterioration in quality of


135 Id.


137 SCHMITT ET AL., supra note 71 at § 2.1.1.4.9.
life for the business. Financial harm does not rise to the level of violent consequence. Therefore, this effect does not cause this action to be classified as an attack.\(^{138}\)

The blackout itself would not be considered an attack because there were no direct violent consequences. The loss of internet access did not inflict death, bodily harm, damage or destruction of property. The hurt felt was minimal. The citizens of Egypt were not able to access the internet and the protestors were not able to communicate using social media sites. This does not rise to the level of violent harm. Thus, this result would not classify this action as an attack.

When Egypt’s government decided to black out the internet to disrupt the protestors, it did not use any form of kinetic force in order to interrupt internet communications. The government used its authority to order the ISPs to shut down services.\(^{139}\) There was no resulting physical damage from the shutdown. Even under the very broadest reading of the term “violence”, the government’s process of cutting off Egyptians from the internet cannot be categorized as violent. The consequences of the method used by the government to limit internet access were also non-violent. Thus, the means used to limit internet access in this situation were not an attack. If the method used to shut down the internet had involved damage of property or

\(^{138}\) John Markoff & Thom Shanker, *Halted ’03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk*, N.Y. TIMES Aug 1, 2009, [http://www.nytimes.com/2009/08/02/us/politics/02cyber.html](http://www.nytimes.com/2009/08/02/us/politics/02cyber.html) (Even though the effects of financial harm would not have been violent, the other possible ramifications of the action would play a role in the decision to use such methods. For example, in 2003 the U.S. government made plans to cyber-attack the Iraqi banking system. The goal was to freeze Saddam Hussein’s assets. The plan was eventually rejected on the grounds that the potential effects of the cyber attack might have spilled over into Europe’s banking systems).

\(^{139}\) Gonsalves, *supra* note 136.
injury to persons then it would have produced violent consequences and been considered an attack.

It is also interesting to note that there has been no accusation from critics that Egypt’s action was an attack. There has been much criticism from many sources but very few have called it an attack, and none in reference to an attack as classified in regards to armed conflict. Criticisms seem to focus on the human rights aspect of the internet blackout. On the day the blackout began White House spokesman Robert Gibbs tweeted, “Govt must respect the rights of Egyptian people & turn on social networking and internet.” That same day, D.C. based Center for Democracy and Technology President Leslie Harris said, “This action is inconsistent with all international human rights norms, and is unprecedented in internet history. Egypt’s actions will only fuel unrest and make peaceful resolution of grievances far more difficult.” The lack of accusations of an attack may stem from the fact that there was no armed conflict in Egypt at the time. However, this as a whole seems to support the conclusion that this type of action would not be considered an attack.

141 Id.
B. Role Reversal, Non-State Actors

The reverse situation, where the protestors block the government’s access to the internet, should be considered as well. A non-state actor would not have the authority to regulate the ISPs and therefore would most likely have to use some sort of violence in order to accomplish the task. In considering the most probable methods to be used by the protestors and the resulting effects it is clear that in most instances the results would have been violent. The five methods to be considered here are the following: cutting the internet cables, blowing up the buildings housing the ISP servers, conducting a cyber-action to take down or damage the servers, an armed takeover of the ISPs, and persuading the ISPs to shut down access voluntarily.

The majority of the internet travel for Europe and Asia passes through the Egyptian fiberoptic corridor.\(^{144}\) Severing these cables would not only affect the internet in Egypt but would also severely affect the internet around the globe.\(^{145}\) That loss or disruption of the internet would not rise to the level of a violent consequence. However, if the protestors damaged or destroyed property in order to sever the connection, then this would be classified as an attack. Most likely the protestors would not have direct access to these cables and therefore would have to damage or destroy part of the cables in order to disconnect them.

If the protestors decided to target the servers of the ISPs instead by bombing the buildings in which they are housed it would be categorized as an attack. The bombings would cause damage and destruction of the servers and surrounding property. There is also a strong possibility that injury and death would result. Each of these outcomes

\(^{144}\) Cowie, supra note 134.
\(^{145}\) Id.
would be a violent consequence of such an action, and accordingly, such action would be an attack.

Using a cyber-operation to take down or damage the servers could be an attack. If the protestors used some tool or program that would cause the servers to shut down without physically damaging them, then the action would not be an attack. However, if a virus or other malware was used that permanently damaged the server in some way, it would be a violent consequence. For example, if the protestors sent a virus that caused the cooling fans in the servers to stop working, leading the servers to overheat and crash, this would be a violent consequence and classified as an attack.

Over-taking the ISPs by force would be an attack. The protestors would be armed and it would be reasonably foreseeable that some type of injury or death, damage or destruction would result from using force to shut down the ISPs. Hence, the results of such an action would be violent and considered an attack.

The only method that on its face would not be an attack would be to persuade the ISPs to voluntarily shutdown internet access. Having the ISPs willingly black out the internet would not involve any damage or destruction of property. It would be similar to having the Egyptian government issue the orders. Remember that the non-state actor (the protestor) is not shutting down the internet out of a matter of right. The Egyptian government had the legal ability to order the blackout. What is proper for a government to do is not always proper for a non-state actor to do. Nonetheless, just because the actor does not have a right does not mean that the action amounts to an attack. There would be no violent consequences as a result of persuading the ISPs to freely shutdown the internet. For that reason, it would not be an attack.

It can be seen from the discussion in this section that Egyptian government’s actions in shutting down the
internet access in Egypt would not be an attack under the law of armed conflict in a non-international armed conflict. Egypt’s actions did not result in any violent consequences. After looking at the situation if the parties had been reversed, it can be seen that most probable methods that could be used by the protestors to limit internet access would likely have resulted in violent consequences and have been classified as an attack.

V. Conclusion

Severing internet access within the borders of a country is not an attack in a non-international armed conflict. An attack is an act of violence. As a result of the blurring between international armed conflicts and non-international armed conflicts this definition applies in both contexts. To determine if an act is an attack, the effects tests should be applied. This test is the most appropriate test to use. The effects test looks at the consequences of the action and determines if the results are violent. Violent consequences are more than just mere inconvenience. They are consequences that result in injury or death, physical damage or destruction to property. When this test is applied to the hypothetical proposed, it can be seen that the Egyptian government’s actions in shutting down the internet did not produce any violent consequences. Therefore, Egypt’s actions of severing internet access within its borders would not be an attack in a non-international armed conflict.
Bitcoin Laundromats for Dirty Money: The Bank Secrecy Act's (BSA) Inadequacies in Regulating and Enforcing Money Laundering Laws over Virtual Currencies and the Internet

By Sheng Zhou*

Abstract:

The Bank Secrecy Act of 1970 is facing the threat of becoming unable to cope with virtual economic transactions. The rise to prominence of virtual worlds and virtual currencies in the last decade has resulted in a move by financial criminals to conduct money-laundering operations on the Internet. One such virtual currency, Bitcoin, operates as a decentralized unit of exchange with a set exchange rate to real world currencies based on supply and demand. However, existing regulations set out by the Bank Secrecy Act do not address virtual economies, leaving the burgeoning e-commerce sector in a legal grey area. Consequently, law enforcement has become increasingly aware of the threat posed by criminals who use Bitcoin and other virtual currencies to launder money outside the scope of the existing law.

This Comment explores the legal history of the Bank

* Mr. Zhou is a third-year J.D. student at American University's Washington College of Law graduating in May 2014, specializing in Corporate Law and Cyberlaw. He received his B.A. from George Washington University, in International Affairs and International Economics. Mr. Zhou can be reached at szhou89@gmail.com or through Twitter at @ShengZhouEsq.
Secrecy Act and its relevance with the growth of the virtual currency, Bitcoin. Furthermore, this Comment seeks to demonstrate the relative ease of using Bitcoin to launder money under existing regulations in comparison to traditional money laundering through a bank. In light of these loopholes, this Comment seeks to make recommendations as to ways the virtual currency legal loophole can be fixed.

I. INTRODUCTION

“The [Federal Bureau of Investigation (FBI)] assesses . . . in the near term, cyber criminals will treat Bitcoin as another payment option alongside more traditional and established virtual currencies . . . and cyber criminals may increasingly use Bitcoins to purchase illegal goods and services and to fund illegal activities.”\(^1\) One of the core “illegal activities” referred to by the declassified FBI report on cybercrimes and virtual currencies is the use of virtual currencies to engage in money laundering to finance criminal activities.\(^2\)

Money laundering is the process of taking the financial proceeds of criminal activity and making them appear legal. Generally, this process involves purposefully

\(^1\) See FBI, BITCOIN VIRTUAL CURRENCY: UNIQUE FEATURES PRESENT DISTINCT CHALLENGES FOR DETERRING ILLICIT ACTIVITY (2012), http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf 5-6 (2012) (making the argument that law enforcement entities such as the FBI must become increasingly aware of the threat posed by Bitcoin, and highlighting the need for third party Bitcoin services to require customers to submit valid identification to complete exchange transactions in order for law enforcement measures to be effective).

\(^2\) Id. at 2 ¶ 5 (“Since Bitcoin does not have a centralized authority, law enforcement faces difficulties in detecting suspicious activity, identifying users, and obtaining transaction records – problems that might attract malicious actors to Bitcoin.”).
mixing illegally acquired money with legally acquired money so that it is difficult to detect and even harder for federal prosecutors to determine its origins.\(^3\) Recent estimates of global money laundering are in the range of 1.6 trillion US dollars in a given year.\(^4\)

In order to combat money laundering, the Group of Seven (G7) created the Financial Action Task Force (FATF), an international body dedicated to eradicating money laundering and terrorist financing to investigate solutions to new money laundering methods. The FATF has led the charge for greater regulation and accountability, offering recommendations to global governments of measures that should be implemented by both formal and informal financial sectors.\(^5\) The organization’s

---


5 See generally FINANCIAL ACTION TASK FORCE, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION (2012), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf [hereinafter International Standards] (the key aspects of the FATF’s recommendations are: identifying all individuals and businesses engaged in financial transactions, both formal and informal; obtaining accurate and verifiable information through which customers can be identified; and maintaining records of all financial transactions and reporting those identified as suspicious to the appropriate authorities); Financial Action Task Force, http://www.fatf-gafi.org/ (follow “About the FATF” hyperlink) (last visited Feb. 10, 2014) (lays out the functions of the FATF as an intergovernmental body created to make and enforce policies regarding international money laundering).
recommendations are adopted universally by members of the Group of 20 (G20) and are reflected in attempts by the U.S. Department of Treasury to curb money laundering in the United States.6

Within the United States, the Bank Secrecy Act of 19707 incorporates most of the FATF’s recommendations. The principal goal of the BSA is to protect the access points to the United States financial system and to safeguard the American banking system from the abuses of financial crime, money laundering, and other illicit monetary activities.8

However, with the growing popularity of the Internet and the rise of global crime syndicates and terrorist groups in the 21st century, the framework of the BSA is no longer enough to keep up with the changing nature of global finance. A major loophole in the BSA is that the BSA’s anti-money laundering provisions do not impose reporting requirements upon financial transactions not involving the physical transfer of currency.9 Congress has

6 See, e.g., Money Laundering Prevention, supra note 3 (showing the implementation of the FATF recommendations in US Treasury requirements for prevention of money laundering).
updated the BSA multiple times since 1970, with the most recent change being in 2001.\textsuperscript{10} The new updates expanded existing BSA regulations by ensuring that all individuals or entities that transfer money, no matter how formal or informal, must comply with all anti-money laundering and counter-terrorist financing regulations.\textsuperscript{11} However, the language of the updates is unclear as to the breadth of the transactions covered, which brings into question its applicability with virtual transactions.\textsuperscript{12}

Under current frameworks, cyberspace and virtual currency exist in a legal grey area. While courts have applied property, tort, and criminal law to disputes over the Internet, those are often over disputes with calculable and foreseeable damages.\textsuperscript{13} However, a distinguishing


\textsuperscript{11} See Shawn Turner, Note, \textit{U.S. Anti-Money Laundering Regulations: An Economic Approach to Cyberlaundering}, 54 CASE W. RES. L. REV. 1389, 1404 (2004) (demonstrating that the PATRIOT Act extended the definition for "financial institutions" to include foreign banks and that the BSA's broadening scope brings vast numbers of institutions within the BSA's coverage).

\textsuperscript{12} See Eric J. Gouvin, \textit{Bringing Out the Big Guns: The USA Patriot Act, Money Laundering, and the War on Terrorism}, 55 BAYLOR L. REV. 955, 982 (2003) (explaining that the PATRIOT Act does not account for “back door” techniques, and that workarounds are therefore possible for criminals and terrorists who really want to circumvent the regulations).

\textsuperscript{13} Accord Susan W. Brenner, \textit{Fantasy Crime: The Role of Criminal Law in Virtual Worlds}, 11 VAND. J. ENT. & TECH. L. 1, 1 (2008) (making the argument that crime on the Internet crosses over into the real world and vice versa, and as a result, cybercrime can and should be
difference with money laundering in cyberspace is the fact that, when done through informal channels, there is often no discernible trail. The versatility and openness of the Internet allows criminals the ability to conduct illicit financial transactions from opposite ends of the world with little to no barriers, creating a legal conundrum regarding enforcement of FATF.\textsuperscript{14}

Consequently, this Comment seeks to examine the plausibility and possibility of legal enforcement of financial transactions using virtual currencies. In particular, it will seek to explain how Bitcoin, a popular virtual currency, operates and how it can be used to money launder over the Internet. The Comment will explore whether current money laundering statutes are and expansive enough for law enforcement authorities to enforce money laundering laws on virtual currencies. To accomplish this task, the Comment will rely on a comparison of two hypotheticals: one being a traditional money-laundering situation via a banking institution and the other being a situation involving the use of Bitcoins to move large amounts of illicit money across the Internet. Finally, this Comment seeks to make recommendations on how money laundering can be prevented with changes to current statutory regulations.

II. MONEY LAUNDERING IN CYBERSPACE: A BACKGROUND

\textsuperscript{14} See, e.g., FINANCIAL ACTION TASK FORCE, MONEY LAUNDERING USING NEW PAYMENT METHODS (2010), http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf, 12-14 (outlining what some jurisdictions, such as the European Union, have done to implement FATF guidelines with regards to newer forms of payment methods).
A. The Bank Secrecy Act of 1970 and its subsequent updates established the basic framework for enforcing the prevention of money laundering within the United States.

To combat money laundering, the government recognized the importance of recording financial transactions, whereby law enforcement officials could trace the origins of large transactions within financial institutions.\(^{15}\) Furthermore, under the BSA, if a banking institution suspected that a financial transaction was illicit, the bank was required to flag the transaction to the U.S. Department of Treasury.\(^{16}\) Banks in the United States were obligated to file Currency Transaction Reports (CTRs) in order to qualify for federal depository insurance, but the CTRs only applied to physical transfers of currency.\(^{17}\)

Since its passage, the Congress has updated the

\(^{15}\) See Straub, supra note 8, at 522-23 (argues that one of the primary policy goals of the BSA was to create formalized procedures for financial records: “The BSA requires all formal financial institutions to file Currency Transaction Reports with the Internal Revenue Service (IRS) when conducting transactions with a single individual exceeding US$ 10,000.”).

\(^{16}\) See, e.g., FinCEN, GUIDANCE ON PREPARING A COMPLETE & SUFFICIENT SUSPICIOUS ACTIVITY REPORT NARRATIVE (2003), http://www.fincen.gov/news_room/rp/files/sar_guidance_narrative.pdf [hereinafter FinCEN SAR] (“The purpose of the Suspicious Activity Report (SAR) is to report known or suspected violations of law or suspicious activity observed by financial institutions subject to the regulations of the Bank Secrecy Act (BSA) . . . information provided in SAR forms also presents the Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN) with a method of identifying emerging trends and patterns associated with financial crimes.”).

\(^{17}\) See, e.g., Baldwin, supra note 9, at 426 (1996) (arguing that none of the provisions go so far as to impose recordkeeping or reporting requirements upon financial transactions which do not involve the physical transfer of currency).
BSA to keep up with the closing of money laundering loopholes. The first major update happened in 1986 with the passage of the Money Laundering Control Act\textsuperscript{18} (MCLA), which explicitly defined the boundaries of the criminalization of money laundering.\textsuperscript{19}

The MCLA was the subject of the Supreme Court decision in Ratzlaf v. United States,\textsuperscript{20} a decision that brought into question the money laundering definitions established by the MCLA. The Supreme Court’s opinion in the case criticized the vagueness of the language of the statute, which prompted Congress to amend the relevant statutory section and pass the Money Laundering Suppression Act (MLSA) of 1994.\textsuperscript{21} The new act made it easier to convict an alleged criminal of money laundering without having to prove that an alleged criminal had actual knowledge that he or she was committing money

\textsuperscript{19} See Scott Sultzer, Money Laundering: The Scope of the Problem and Attempts to Combat It, 63 TENN. L. REV. 143, 166-168 (1995) (stipulating that knowingly helping launder money derived from criminal activity; knowingly engaging in transactions exceeding U.S. $10,000 that involve property from criminal activity; and knowingly structuring transactions to avoid BSA reporting were deemed to be money laundering criminal offenses).
\textsuperscript{20} See Ratzlaf v. United States, 510 U.S. 135, 114 S. Ct. 655 (1994), superseded by statute, (deciding in a 5-4 decision, the Court held that the willfulness component of § 5324 requires the Government to prove that the defendant had knowledge that his actions were illegal and that Congress could have, but failed to, explicitly dispense with the willfulness requirement in the statute); see also United States v. Caro, 454 Fed.Appx. 817, 839 n.24 (11th Cir. 2012) (highlighting the statutory amendment to § 5324 in the aftermath of Ratzlaf to narrow the requirement to convict under the standard of willful knowledge, which renders the substantive decision in Ratzlaf moot).
\textsuperscript{21} Money Laundering Suppression Act, Pub. L. 103–325, title IV, § 401 (Sept. 23, 1994).
The view of law enforcement towards money laundering and the BSA changed dramatically after September 11, 2001. As part of Title III of the USA PATRIOT Act, Congress passed the International Money Laundering Abatement and Anti-Terrorist Financing Act (IMLAF) of 2001 to combat the use of money laundering by terrorist organizations, namely through informal transactions. For the first time, IMLAF expanded the jurisdiction of the BSA to all financial transactions, formal and informal, and required informal money transfers to conform to the BSA financing regulations. As opposed to formal financial institutions, which are mainly banks who conduct wire transfers, informal financial institutions are generally underground financial networks, collectively

22 See, cf., Jeremy Sanders & Jennifer Smolansky, Financial Institutions Fraud, 41 AM. CRIM. L. REV. 671, 719 (2004) (arguing that although the MLSA removed the willful knowledge requirement, the requirement that the alleged criminals knowingly were engaging in illegal conduct still stands).
23 PATRIOT Act, supra note 10.
24 See id. §§ 301-377 (2001) (recognizing the need to ensure that all appropriate elements of the financial services industry are subject to appropriate requirements to report potential money laundering transactions to proper authorities).
25 See Andres Rueda, International Money Laundering Law and Enforcement and the USA Patriot Act of 2001, 10 MSU-DCL J. INT'L L. 141, 150-152 (2001) (laying out examples of informal financial institutions that are now covered under the BSA due to the IMLAF, which include: money transmitters, check-cashing companies, jewelers, pawn brokers, casinos, credit-card companies, and issuers of traveler's checks and money orders); see also Turner, supra note 11, at 1404 (pointing out that IMLAF extended the definition for "money transmitter" to include any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money).
referred to as “Informal Value Transfer Systems” (IVTS).\textsuperscript{26} These IVTS exist outside of the modern banking system and serve as an alternative to people who either do not have access to or prefer not to use the formal banking system. However, IVTS do serve a similar purpose to that of the formal systems, which is to facilitate the transfer of valued goods and money.\textsuperscript{27}

Under the language of the IMLAFA, IVTS are referred to as “money transmitters” or “money services businesses” (MSB).\textsuperscript{28} However, it is unclear whether

\textsuperscript{26} See, e.g., NIKOS PASSAS, INFORMAL VALUE TRANSFER SYSTEMS & CRIMINAL ORGANIZATIONS: A STUDY INTO SO-CALLED UNDERGROUND BANKING NETWORKS, WODC Onderzoeksnotitie(s) (1999), available at http://english.wodc.nl/images/on1999-4-full-text_tcm45-56889.pdf (arguing that IVTS is a system or network of people facilitating, on a full-time or part-time basis, the transfer of value domestically or internationally outside the conventional, regulated financial institutional systems); see also Courtney J. Linn, One-Hour Money Laundering, 8 U.C. DAVIS BUS. L. J. 138, 138 (2007) (discussing the lowered standard of scrutiny given to IVTS as compared to banks due to the wide variety of IVTS and difficulties in regulation).

\textsuperscript{27} See, e.g., FINCEN, INFORMAL VALUE TRANSFER SYSTEMS (2003), http://www.fincen.gov/news_room/rp/advisory/pdf/advis33.pdf (stating that IVTS are generally accessible around the world, even in some of the most politically unstable regions, and are reliable, efficient, and most importantly, anonymous).

\textsuperscript{28} PATRIOT Act, supra note 10, § 359(b) (amending the BSA to include the clause “or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system”); see also FinCEN: Am I an MSB?, http://www.fincen.gov/financial_institutions/msb/amimsb.html (last visited Feb. 10, 2014) [hereinafter FinCEN MSB] (stating that MSBs are grouped into five distinct types of financial services providers: currency exchangers; check cashers; issuers, sellers, or redeemers of traveler’s checks, money orders or stored value; the United States Postal Service; and money transmitters).
virtual currency transactions would fall under the definition of a MSB under the updated BSA guidelines.

B. Since the passage of the BSA, technology has updated significantly with the advent of digital currency and the global use of the Internet.

Virtual worlds arose with the proliferation of the Internet in the mid to late 1990s. They exist in parallel to the real world, and users can remotely and simultaneously access them with the use of a computer and an Internet connection. Because virtual worlds mirror the real world, many have virtual economies. This allows users to not only connect with one another, but also to conduct financial transactions. A recent court decision involving the legal status of virtual currencies took the approach that virtual currencies are similar to that of real currencies.

---

29 See Beth Simone Noveck, The State of Play, 49 N.Y.L. SCH. L. REV. 1, 10 (2004) (making the argument that virtual worlds are becoming similar to real life and emulate societal norms in reality).

30 Id. at 11 (pointing out that three-dimensional physical, interactive, and immersive spaces can be called "virtual reality" in a way that was never applicable for a simple Internet interface).

31 See, e.g., Posting of Brad Plummer to Wash. Post Wonkblog, http://www.washingtonpost.com/blogs/wonkblog/ (Sep. 28, 2012, 8:30 PM) (exploring the economies of several online video games and the mirroring of real-world economies in these virtual worlds where users can use virtual world currencies to purchase property within that virtual world and in the real world).

The ability to conduct real-time, in-world transactions in virtual currency that can then be exchanged for real world money has made virtual economies a thriving medium of financial transactions. The ability of users to transfer money directly from bank accounts to virtual accounts highlights the growing interconnectivity between real world financial institutions and virtual currencies.33

No virtual currency currently is more versatile, liquid, and convertible than a virtual currency unit known as Bitcoin. Bitcoin was created by a group of computer programmers who wanted to create a virtual currency for the Internet community as a whole.34 The premise behind Bitcoin was to create a decentralized Internet currency where government involvement is forbidden and unnecessary.35 To that end, Bitcoin came to fruition in 2009, based on peer-to-peer technology (P2P), meaning that Bitcoin is completely decentralized and reliant on users

33 See Mayer-Schönberger & Crowley, supra note 32, at 1777, 1787 (pointing out that over 380,000 distinct objects changed hands in the month of July 2006 in ten million user-to-user transactions, which yielded an internal economy of US $ 10 million for that month).


35 See, e.g., Wei Dai: B-Money, http://weidai.com/bmoney.txt (last visited Feb. 10, 2014) (outlining the core philosophical principle that in a crypto-anarchy, the government is forbidden and permanently unnecessary in regards to backing Bitcoin).
for transactional management and distribution. Unlike real world currencies, whose value is derived through regulation or law and backed by the state, Bitcoins have no intrinsic value due to their composition from binary numbers rather than precious metals, and their pricing is determined solely by economic supply and demand.

While this may seem like a recipe for mass replications of Bitcoins, that is not the case. There is a finite amount of Bitcoins in existence at any given time, created through a process known as mining, and the law of diminishing returns applies. Mined Bitcoins are stored as computer files on a user computer, but are logged on a global public ledger. This public record is kept using a P2P network connected to the Bitcoin network, operated and

36 See, e.g., Wallace, supra note 34 (explaining the origins of Bitcoin and the initial framework of the founders to create a currency that had no central governing body).
37 See, e.g., Posting of J.P. to Babbage Blog, http://www.economist.com/blogs/babbage/ (Jun. 13, 2011, 208:30) (stating that the difference between fiat currencies and Bitcoin is that real world currencies, in principle, are answerable to its citizens, while Bitcoins comprise a community currency that is self-policing on the part of its users).
38 See Andy Greenberg, Crypto Currency, FORBES, May 9, 2011, http://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html (highlighting that Bitcoin's distributed software is set to slow production over time so that there will never be more than 21 million Bitcoins in circulation); see also Ogashi Tukafoto, Bitcoin Mining for Fun and Net Loss, SLACKTORY, Aug. 4, 2011, http://slacktory.com/2011/08/bitcoin-mining-fun-loss (stating that the rewards for Bitcoin mining get smaller and the incentive to mine switches to an incentive for collecting small transaction fees and keeping the network secure by verifying network transactions).
maintained by thousands of home computers. This ledger automatically updates every time there has been a transactional exchange of Bitcoins between users. The whole process is transparent to both parties involved in the transaction and allows the parties to deal directly with one another without a third party having to authorize the transaction. This ensures security as well as anonymity in transactions between users.

The mining process involves the use of special software by a Bitcoin miner that solves randomly generated complex math equations. However, the problems are so complex that they usually require the resources of complete networks of computers to compute any given problem. The program also caps the amount of Bitcoins that can be generated within a given period, creating a sense of

39 See, e.g., Barrett Sheridan, Bitcoins: Currency of the Geeks, BLOOMBERG BUSINESSWEEK, June 16, 2011, http://www.businessweek.com/magazine/content/11_26/b4234041554873.htm (pointing out that individual transactions are encrypted, logged by a decentralized network running on thousands of home computers, and recorded in a public ledger similar to a peer-to-peer network for file sharing).

40 E.g., J.P., supra note 37 (arguing that by placing the records in a P2P network, transactions are effectively secure from manipulation due to the multiple copies of the records existing on millions of computers worldwide, encrypted by public-key encryptions, ensuring the currency’s security); see also Bitcoin Wiki: Mining, https://en.bitcoin.it/wiki/Mining (last visited Feb. 10, 2014) (stating that the ledger of past transactions is called a block chain and serves to confirm transactions to the rest of the network as having taken place, validating the legitimacy of Bitcoins in circulation).

41 See, e.g., Sheridan, supra note 39 (pointing out that the greater the computing power, the more Bitcoins that can be generated).

42 See Greenberg, supra note 38 (stating that the machines in Bitcoin's mining network compute an encryption function called a "hash" on a set of random numbers, and coins are awarded when a user computes the right number chain. However very few people obtain the correct chain, thus limiting the number of coins awarded).
stability for the value of Bitcoin.\footnote{See, e.g., Jon Radoff’s Internet Wonderland, \url{http://radoff.com/blog/} (June 3, 2011) (postulating that running a mining operation on Bitcoin is similar to buying into the lottery, where computing power is exchanged for a chance to obtain Bitcoins).}

Due to the prohibitively difficult nature of Bitcoin mining, most people obtain Bitcoins from Bitcoin exchange sites. Several websites provide services for the exchange of Bitcoins based on market prices of Bitcoin against real world currencies.\footnote{See Greenberg, supra note 38 (stating that about $30,000 worth of Bitcoins change hands every day in electronic transactions, spent on Web-hosting, electronics, and other commodities).} Different websites offering Bitcoin exchanges and purchases have different policies for conducting the transaction.\footnote{See, e.g., Daniel Lyons, The Web’s Secret Cash: A Novel Version of Money is Sprouting Online, Letting People Shop In Complete Anonymity, NEWSWEEK, June 19, 2011, \url{http://www.thedailybeast.com/newsweek/2011/06/19/the-web-s-secret-cash.html} (illustrating the free market nature of the Bitcoin trading price, which fluctuates based on demand and can range widely in value).} Before its closure under acrimonious circumstances in February 2014, the most popular Bitcoin exchange site was a website called MtGox. On this site, a user needed to add a state-backed currency to his or her account. Then the user could directly buy Bitcoins from MtGox using money in the linked bank account.\footnote{See generally MtGox, \url{https://www.mtgox.com/} (last visited Feb. 10, 2014) (outlining the function of the service and requirements that are needed to have an account on MtGox and to engage in financial transactions using the website).} Despite the requirement of linking a bank account or Paypal account, the website facilitated exchanges in relative anonymity.\footnote{E.g., Bitcoin Wiki: MtGox, \url{https://en.bitcoin.it/wiki/MtGox} (last visited Feb. 10, 2014) (stating that MtGox operates as a facilitator of exchange of Bitcoins between users and not as an overseer or regulatory agent).} Other websites even...
offer to facilitate transfers of Bitcoins in person, organizing face-to-face meetups for people interested in doing so.48 Today, many websites, and even real world stores, accept Bitcoins as legal currency in exchange for goods and services.49

C. While the typical fact patterns for money laundering through traditional methods and through using Bitcoins are similar, there are major differences in the ability of law enforcement to track down the culprits.

In the first scenario, a crime syndicate, in order to launder their illegally obtained money, makes six deposits with a multinational Bank A, with branches in the US. One deposit is $12,000, while the other five were below $10,000, totaling $35,000 worth of deposits. The deposit of $12,000 was not split into smaller denominations. While the bank allowed the deposits to be made, the deposit of $12,000 triggered the requirement for the bank to file a

48 See, e.g., Trade Bitcoin: Local Trading, http://tradebitcoin.com/about/ (last visited Feb. 10, 2014) (portraying the service provided by the website as a facilitator of face-to-face meetings of Bitcoin exchanges for people in a user’s area).
49 See Psuedonymous, I Spent a Coin (and I Liked It) — How I Bought Lunch With Bitcoins, NYMAG, June 28, 2011, http://nymag.com/daily/intelligencer/2011/06/i_spent_a_coin_and_i_liked_it.html (detailing how the author bought lunch at a local New York City restaurant using Bitcoins and illustrates the growing acceptance of Bitcoins as another form of currency); see also The Tuesday Podcast: Bitcoin (NPR Planet Money podcast Jun. 12, 2011), http://www.npr.org/blogs/money/2011/07/13/137795648/ (explaining the increasing use of Bitcoins within the US to purchase goods and services online and in the real world).
CTR to the IRS. The bank did not fill out a Suspicious Activity Report with the CTR and the deposits were processed.

A week after the criminal syndicate made the deposits, they transferred the deposits into two offshore Cayman Island banks, and then back to another American bank, Bank B. The withdrawal of the $12,000 prompted another CTR to be filed by Bank A and the deposit of $12,000 a week later to Bank B prompted Bank B to file another CTR. At this stage, three CTRs have already been submitted to the IRS by two American banks. The close proximity of these transactions alerted the government and the FBI began to investigate the transactions. The FBI determined that the $12,000 dollars had routed between several offshore accounts between Bank A and Bank B. The pattern of the money


51 See, e.g., FinCEN SAR, supra note 16, at 1 (stating that Suspicious Activity Reports are only required to be filled and submitted along with a CTR if the financial institution has reason to believe that the transaction involved suspicious funds).

52 See Sultzer, supra note 19, at 148-151 (outlining the steps of a traditional money laundering operation, involving rerouting the funds through other banks as a common method to escape detection from law enforcement and to make the money seem legitimately derived from different sources).

53 See, e.g., Baldwin, supra note 9, at 441 (1996) (postulating that FinCEN uses artificial intelligence to aid in the identification of money launderers by analyzing a compilation of data, including CTR's, to identify and monitor potentially illegal patterns of behavior characteristic of money laundering).
points towards a potential money-laundering situation.\textsuperscript{54}

A week after investigations started, the FBI noticed that money from six accounts at Bank B, which had arrived around the same time, one of which was the $12,000 account, began to be withdrawn. Agents obtained a warrant and detained the men who were making the transactional withdrawals from Bank B. The agents were able to ascertain to a reasonable extent that the laundered money came from an illegal meth operation. On top of all the other criminal charges, the FBI wants to charge the defendants under the Bank Secrecy Act for money laundering.\textsuperscript{55}

In the second scenario, another criminal syndicate has made the decision to turn to a far more lucrative and accessible way to money launder, by using virtual currency. They decided that Bitcoin was the best way to quickly and anonymous launder tens of thousands of dollars of cash from their illegal operations. A syndicate member created several accounts on MtGox and linked these accounts to his Dwolla account.\textsuperscript{56} Fifty thousand dollars’ worth of illegally acquired funds were put in his Dwolla account and used as the basis for his transactions on MtGox. Assuming that the exchange rate of Bitcoins to US Dollars was 1 BTC

\textsuperscript{54} See Rueda, supra note 25, at 164 (detailing the assistance of FinCEN guidelines in helping law enforcement officers and prosecutors initiate and facilitate investigations into money laundering).

\textsuperscript{55} See 18 U.S.C. § 1957 (2006), available at http://www.law.cornell.edu/uscode/text/18/1957 (stating that prosecutors have to know that they can prove the members involved in the laundering operation knowingly engaged or attempted to engage in a monetary transaction in criminally derived property of a value greater than $10,000).

\textsuperscript{56} See, e.g., Dwolla, https://www.dwolla.com/about (last visited Feb. 10, 2014) (explaining that Dwolla is a cash based payment network that can be used to buy goods and services online, similar to Paypal, but without the need to link the account to a formal financial institution).
for $20,\textsuperscript{57} he was able to successfully purchase 2,500 Bitcoins from other users around MtGox. After purchasing these Bitcoins, he proceeded to use the same website to sell off his 2,500 Bitcoins.\textsuperscript{58} Over the course of the month, the he was able to sell all his coins, at a minor profit, due to unusually higher demand for the coins. He then withdrew about $52,000 from his Dwolla account.\textsuperscript{59}

Posing as a Bitcoin buyer, federal agents had been watching MtGox for unusually large transfers of Bitcoins. The purchase of 2,500 Bitcoins across several accounts and the instant resale of these Bitcoins raised suspicions among federal investigators. However, due to the highly anonymous nature of transactions with Bitcoin, the investigation could not produce the names and locations of the buyers and sellers.\textsuperscript{60} Since data regarding each client is stored locally and not in a central server, attempts to subpoena MtGox would not produce anything to help federal investigators.\textsuperscript{61} However, during the transaction with one of the launderer’s accounts, FBI agents were

\begin{flushleft}
\textsuperscript{57} Accord Coinmill.com: The Currency Converter, https://coinmill.com/BTC_USD.html (last visited Mar. 1, 2014) (showing the current exchange rate between USD and BTC to be around $613.90 to 1 BTC).
\textsuperscript{58} See Bitcoin Wiki: MtGox, supra note 47 (giving instructions on how users can buy and sell on MtGox using Dwolla as a cash basis for all their transactions).
\textsuperscript{59} See, e.g., Dwolla, supra note 56 (advertising the fluidity and ease of moving cash around with the Dwolla service).
\textsuperscript{60} See, e.g., Greenberg, supra note 38 (illustrating that there is no centralized storage of funds, so accounts cannot be frozen by authorities such as law enforcement or PayPal administrators).
\textsuperscript{61} See, e.g., Sheridan, supra note 39 (stating that individual transactions are encrypted, logged by a decentralized network running on thousands of home computers, and recorded in a public ledger).
\end{flushleft}
successful in obtaining his IP Address, which indicated that the seller was based in the United States.

III. RECENT UPDATES TO THE BSA DO NOT ENCOMPASS TRANSACTIONS INVOLVING DIGITAL CURRENCY, CREATING SCENARIOS WHERE ILLEGAL ACTIVITIES CAN OCCUR WITHOUT REGULATION.

Despite the recent attempts by FinCEN to encompass internet transactions under the umbrella of MSBs, Congress has not updated the statutory framework since 2001. At present, the broad academic nature of the definition of IVTS and MSB does not allow for a clear legal delineation of whether virtual currency transactions fall under the definitions of the BSA. Furthermore, the pseudonymous nature of Bitcoin means that investigators have very limited means to track Bitcoin transactions. Even if the FBI was aware of major money-laundering operations happening through the usage of Bitcoin exchange sites, there is very little that they can do to track

---

62 How Stuff Works: What is an IP Address?, [http://computer.howstuffworks.com/internet/basics/question549.htm](http://computer.howstuffworks.com/internet/basics/question549.htm) (last visited Feb. 10, 2014) (explaining that an Internet Protocol address (IP) is registered to an individual computer as it is connected to the Internet in a given session, similar to a home address).

63 See Posting of Dennis Lormel on Counterterrorism Blog, [http://counterterrorismblog.org/2008/05/two_easily_exploitable_vulnerabilities.php](http://counterterrorismblog.org/2008/05/two_easily_exploitable_vulnerabilities.php) (May 21, 2008, 15:41 EST) (reaffirming that MSBs refer to five distinct types of financial services providers and nothing more).
down the source of transactions.64 This is highlighted by the recent closure of MtGox and the purportedly missing $450 million worth of Bitcoins, demonstrating the limited ability of the authorities, and even the site administrators, to track and locate Bitcoins when they seemingly vanish into the Internet.65

The current framework is inadequate in preventing cyber laundering because it does not directly acknowledge the existence of virtual currencies and a clear definition.66 In analyzing the factual hypotheticals posited in the last section, it becomes clear that the existing legal framework is appropriate for traditional money laundering, but is inadequate in addressing money laundering using virtual

64 See Thomas Lowenthal, *Bitcoin: inside the encrypted, peer-to-peer digital currency*, ARS TECHNICA (Jun. 8, 2011) http://arstechnica.com/tech-policy/2011/06/bitcoin-inside-the-encrypted-peer-to-peer-currency/ (pointing out that Bitcoins can be as anonymous as the user wants); but see Jon Matonis, *Bitcoin’s Greatness Not Realized By Succumbing To Regulation*, FORBES (Dec. 9, 2012) http://www.forbes.com/sites/jonmatonis/2012/12/09/bitcoins-greatness-not-realized-by-succumbing-to-regulation/ (arguing that Bitcoin users prefer the anonymity of Bitcoin and that the self-regulating nature of Bitcoin does not require the government to step in and regulate the transactions); but see Sarah Meiklejohn, et. al., *A Fistful of Bitcoins*, 38 ;LOGIN: 6 (December 2013) http://cseweb.ucsd.edu/~smeiklejohn/files/login13.pdf (demonstrating the potential deanonymization techniques that law enforcement could use to locate stolen Bitcoins).


66 See, e.g., Straub, *supra* note 8, at 527 (2002) (pointing out that existing regulations create a system to report transactions that occur in financial transactions, but the very nature of e-money is that there is little to no reporting requirement).
currencies. However, in order to bring virtual currencies into the realm of governmental regulation, it will be necessary to confront privacy issues and fundamental changes in the way the government treats the Internet.  

A. U.S. law enforcement’s awareness of the potential threat of the use of virtual currencies, such as Bitcoin, to launder money outside the scope of existing law illustrates a current inadequacy in regulation.

At its core, Bitcoin fits within the parameters of an IVTS, and with its decentralized nature and its mobility, it creates the ability to move large amounts of money at once without triggering BSA safeguards. While it does not explicitly fall within any category of the IMLAFA definition of a MSB, it is clear that Bitcoin is an informal

---


financial institution. 69 Consequently, under the murky definition of MSBs as established by the IMLAFA, how would Bitcoin fare under attempts by law enforcement to enforce BSA standards on Bitcoin transactions? If the government does manage to hold someone accountable for money laundering using Bitcoins, they must prove the presence of three elements, as outlined by the BSA. 70

Attempts by the US Department of Treasury to strengthen the definitions of MSB to include greater variations of IVTS, 71 along with an FBI report highlighting the threat posed by cyber criminals, seem to illustrate the reality of the threat of money laundering using virtual currencies and the inability of current regulations to address the concerns of virtual money laundering. 72

B. The current BSA rules would be able to regulate and enforce anti-money laundering laws in a case of

69 See, e.g., Bitcoin Money: FinCEN Brings KYC Requirements to Bitcoin?, http://www.bitcoinmoney.com/post/8412471372/fincen-prepaid-access-final-rule (last visited Feb. 10, 2014) [hereinafter FinCEN KYC] (including the possibility that even businesses outside the U.S. conducting money transfer over the Internet could still be classified as U.S. MSBs and that the definition no longer requires that a MSB be a business, but can be any individual who receives funds in exchange for a stored value might be considered an MSB).

70 See U.S. v. Carucci, 364 F.3d 339, 343 (1st Cir. 2004), available at https://www.casetext.com/case/us-v-carucci/ (“(1) the defendant engaged or attempted to engage in a monetary transaction with a value of more than $ 10,000; (2) the defendant knew that the property involved in the transaction had been derived from some form of criminal activity; and (3) the property involved in the transaction was actually derived from specified unlawful activity.”).

71 See, e.g., FinCEN KYC, supra note 69 (pointing towards the new ruling from FinCEN that attempts to expand the definition of MSB to encompass more IVTS).

72 See generally FBI, supra note 1 (outlining that the FBI views cyber criminals who use virtual currencies to money launder using the Internet as a potential threat).
money laundering using formal financial institutions.

Under traditional money laundering, there are usually three steps: placement, layering, and integration. Placement involves changing the money from criminal activities into a less suspicious form, most commonly with a deposit at the bank. Layering involves the wire transfer of funds from numerous accounts to other accounts in an attempt to hide the funds’ true origins. Integration, the final step, involves movement of the layered funds, their origins no longer traceable, into the global financial world, where the launderers dilute the dirty money with legitimate money.

The federal government has jurisdiction to press charges against the defendant as long as the government

---

73 See, e.g., Money Laundering Prevention, supra note 3 (stating that the focus of FinCEN’s strategy is to stop money launderers at the placement stage, before the layering process can disguise the funds’ origin).

74 See Sultzer, supra note 19, at 148 (illustrating that the placement stage of money laundering is the hardest stage for money launderers to commit and that launderers will often route cash through a front operation in order to give the funds a legitimate cover when they are deposited into a financial institution).

75 Id. at 150 (highlighting the fact that layering is the process where the origins of the funds being laundered are masked through dispersions to other banks, usually outside the United States).

76 Id. at 151 (stating that funds are integrated into the legitimate financial world through forms such as letters of credit, bonds, and other securities, prime bank notes and guarantees); accord Greg Dekermenjian, Developments In Banking And Financial Law: 2005: Xiv. Anti-Money Laundering, 25 ANN. REV. BANKING & FIN. L. 137, 141-143 (2006) (arguing that traditional money laundering laws has extensive programs to prevent acts of money laundering happening in formal financial institutions).
has enough evidence to press for a case.\(^{77}\) The bigger question is whether the government will have fulfilled the three elements, as stipulated by the BSA, to convict the defendants of money laundering. In order to find the defendants guilty, the government must prove the existence of all three elements: (1) the defendant engaged or attempted to engage in a monetary transaction with a value of more than $10,000; (2) the defendant knew that the property involved in the transaction had been derived from some form of criminal activity; and (3) the property involved in the transaction was actually derived from specified unlawful activity.\(^{78}\)

Element one is fulfilled with the deposit and withdrawal of the $12,000 in Bank A, as certified by Bank A’s CTRs. Bank B’s CTR can also corroborate the fact that a defendant engaged in a financial transaction above $10,000. Assuming the FBI investigation has some form of evidence linking the defendant to the crime syndicate and that the FBI reasonably believed that the $12,000 came from the drug operation, the crime will also fulfill the second element of the statute. It would seem unlikely for the FBI to pursue a case if there was insufficient evidence


\(^{78}\) See, e.g., 18 U.S.C. § 1957, supra note 55 (ruling that the statute not only lays out the general elements, but also defines a ‘monetary transaction’ as “deposit, withdrawal, transfer, or exchange, in or affecting interstate or foreign commerce, of funds or a monetary instrument’ in § f); see also U.S. v. Carucci, supra note 70, at 343 (reaffirming the First Circuit’s interpretation of the language of 18 U.S.C. § 1957 with regards to the elements that the government has to prove in order to invoke a conviction for money laundering).
as to this regard. Element three is closely linked with element two and, assuming the FBI has evidence or testimony linking the money to the meth operation, then this element is fulfilled.

With all three elements fulfilled, the Department of Justice will most likely win in a court against the defendant. The government could charge the other defendants who were not directly engaged in the $12,000 transaction with at least conspiracy to commit money laundering, but the case against the primary defendant of money laundering in violation of the BSA is straightforward. This result is not surprising as the legislative intent of the BSA was to stop this form of money laundering through formal financial institutions.

C. Money laundering using Bitcoin is a definite possibility, as the nature of Bitcoin allows money launderers to remain anonymous and difficult for law enforcement to detect, and current legislation appears to be inadequate in linking virtual money launderers to the crime.

Assuming that federal prosecutors are held to the

---

79 Id. (pointing out that the fulfillment of all three elements of money laundering in the statute constitutes a violation of the BSA and a money laundering crime).

80 See 18 U.S.C. § 371 (2006) available at http://www.law.cornell.edu/uscode/text/18/371 (“If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both.”).

81 See, e.g., Rueda, supra note 25, at 201 (arguing that the PATRIOT Act strengthens the U.S. financial transaction reporting system to levels never seen before and that the language is very broad in scope).
same standard as they are for formal financial transactions, they must look at the three elements required by the BSA to prosecute the syndicate member for money laundering.82 Despite the expansion of the BSA under IMLAFA to informal transfers, virtual currencies exist in a legal grey area concerning classification.83 Under the definition of MSBs that was set out in IMLAFA, the category that a Bitcoin service like MtGox would fall under would most likely be considered to be either a currency exchanger or money transmitter.84

However, this classification in itself is not completely accurate of the service that MtGox provides for its users. Prosecutors could attempt to explain that MtGox would fall under either of those categories, but they would have to prove that the primary purpose of MtGox is to exchange currencies and/or to transfer money between people.85 This classification is tenuous at best, as MtGox only facilitates the exchange of Bitcoins, units that are not statutorily real currency and are unregulated by the

82 See, e.g., U.S. v. Carucci, supra note 70, at 343 (reiterating the three requirements created by Congress with the passage of IMLAFA in order for a defendant to be convicted for money laundering).
83 See, e.g., FinCEN KYC, supra note 69 (stating that FinCEN is attempting to expand MSBs to encompass virtual currencies, current statutory law remains outdated to address virtual currencies).
84 See, e.g., FinCEN MSB, supra note 28 (laying out the current legal parameters of what is defined to be a MSB, and thus under the regulatory framework of the BSA to be narrow in scope and not all encompassing).
85 See, e.g., Bitcoin Wiki: MtGox, supra note 47 (explaining that MtGox operates as a facilitator of exchange of Bitcoins between users, does not have an overseeing role in transactions, and does not require detailed personal information from users).
government. Furthermore, even if prosecutors were successful in classifying the transactions to be within the purview of the BSA, they would have a difficult time in proving all three elements required to convict for money laundering under the BSA. The only element that could be proven with certainty is that transactions over $10,000 were made, but due to the anonymous nature of the Bitcoins exchange process, it would be near impossible to prove that the money was from illegal sources without help from a third party source, like an informant.

Most likely, without the legal backing of formally declaring virtual currencies to be an IVTS, it is highly unlikely that prosecutors can make the argument that MtGox is a MSB. Consequently, because of this tenuous connection between MtGox and its classification as a MSB, it would seem likely that MtGox would not fall within the

87 See 18 U.S.C. § 1957, note 55 ((1) the defendant engaged or attempted to engage in a monetary transaction with a value of more than $10,000; (2) the defendant knew that the property involved in the transaction had been derived from some form of criminal activity; and (3) the property involved in the transaction was actually derived from specified unlawful activity).
88 See Lowenthal, supra note 64 (pointing out that Bitcoin transactions can be as anonymous as the user wants and the process does not require the registration of a real name and address).
89 See, e.g., FinCEN MSB, supra note 28 (illustrating the conundrum that it would be very difficult to classify what service MtGox would be considered to facilitate, especially with the tricky legal status of Bitcoin as a whole).
reach of the BSA and its regulations.\(^90\) While the deposit of proceeds made from Bitcoin laundering through traditional bank accounts may potentially allow investigators to locate the identities of the virtual money launderers, the patterns attributed to traditional money laundering are not present.\(^91\) Bitcoin-laundered money would appear to be legitimate when deposited into bank accounts, as funds would not be arriving from other banking institutions, but from an online source.\(^92\) Banks will still file CTRs regarding their deposits, but the necessary paper trail to spot money laundering does not exist prior to the transfer of money from a virtual account to a bank.\(^93\) Consequently, deposits made from the proceeds of the Bitcoin exchanges into conventional banking institutions would trigger a CTR, but would be unlikely to raise suspicion due to the direct nature of the

---

\(^{90}\) Compare id. (stating that MSBs are grouped into five distinct types of financial service providers: currency exchangers; check cashers; issuers, sellers, or redeemers of traveler’s checks, money orders or stored value; the United States Postal Service; and money transmitters) with Bitcoin Wiki: MtGox, supra note 47 (explaining that MtGox operates as a facilitator of exchange of Bitcoins between users, which does not seem to fit into the definition of an MSB as laid out by FinCEN).

\(^{91}\) See, e.g., Money Laundering Prevention, supra note 3 (highlighting that the current strategy towards catching money launderers is to stop money laundering at the first stage, before origins of funding can be masked).

\(^{92}\) See, e.g., Dwolla, supra note 56 (explaining that Dwolla exists as a virtual bank account from which money can be drawn to conduct Bitcoin transactions).

\(^{93}\) See, e.g., Sultzer, supra note 19, at 150 (highlighting the fact that layering is the process whereby the origins of the funds being laundered are masked, but the funds retain a paper trail of transactions between banks).
transactions from virtual account to bank account.\textsuperscript{94}

Furthermore, investigators would be unable to bind websites like MtGox to BSA limitations due to the legal grey area in which MtGox operates, with its unclear MSB status.\textsuperscript{95} Consequently, the money launderers would most likely escape without facing formal charges.\textsuperscript{96} The patterns presented demonstrate that the use of Bitcoins to launder money attacks is more than merely a theoretical academic discussion.

\textbf{D. Traditional money laundering schemes and Bitcoin laundering schemes are similar in their intents, but are clearly different in their implementations and regulations.}

At its core, money laundering with Bitcoins is similar to that of laundering through formal banking institutions. Both are means to the same end: to dilute the legality of illegally acquired money.\textsuperscript{97} Their divergence in regulation is a purely legal one. Governments regulate

\begin{footnotesize}
\textsuperscript{94} See, e.g., Greenberg, supra note 38 (illustrating that no paper trail exists for transactions that occur using virtual accounts such as Paypal beyond the immediate transaction in or out of the account).
\textsuperscript{95} See Lormel, supra note 63 (reaffirming that MSBs refer to five distinct types of financial service providers and nothing more).
\textsuperscript{96} Accord Daniela Rosette, \textit{The Application Of Real World Rules To Banks In Online Games And Virtual Worlds}, 16 U. MIAMI BUS. L. REV. 279, 302 (2008) (arguing that in order for any form of regulation to be effective, it requires the tracking of money flows and logging of transactional activity, requirements Bitcoin does not meet).
\textsuperscript{97} See, e.g., Stephen I. Landman, Note, \textit{Funding Bin Laden’s Avatar: A Proposal for The Regulation Of Virtual Hawalas}, 35 WM. MITCHELL L. REV. 5159, 5162 (2009) (making the argument that terrorists using virtual worlds and virtual currencies to money launder to finance their operations are able to do so under the current framework); see also Rueda, supra note 25, at 141 (the goal of traditional money laundering is to make illegal funds seem legitimate).
\end{footnotesize}
formal banking institutions far more due to decades of experience dealing with financial crimes that occur through those channels. All statutory updates passed by Congress since the passage of the BSA were primarily to deal with traditional formal money laundering through formal financial institutions. However, with the advent of the Internet within the last twenty years, the law has yet to keep up with developments on the Internet. The classifications of MSBs under the IMLAFA update to the BSA were made with traditional informal financial transfers in mind, not with the idea of combatting cybercrimes. Consequently, this discrepancy between the reality of vibrant Internet transactions and the legal definition of IVTS creates a legal blind spot, which legally-aware criminals can easily exploit.

98 See Duncan E. Alford, Anti-Money Laundering Regulations: A Burden on Financial Institutions, 19 N.C.J. Int'l L. & COM. REG. 437, 466-467 (1994) (postulating that due to strict regulations and experiences with money laundering in formal financial institutions, launderers are using informal institutions to conduct money laundering).

99 See Landman, supra note 97 (arguing the inadequacy of the current state of the law regarding virtual money laundering and pointing out that existing BSA regulations allow for loopholes that can be exploited by terrorists and criminal organizations).

100 See, e.g., 31 U.S.C. § 5312(a)(2), available at http://www.law.cornell.edu/uscode/text/31/5312 (defining the scope of ‘financial institutions’ under BSA); see also Straub, supra note 8, at 533 (arguing that in order to curb new techniques in money laundering while simultaneously promoting technological development, the government should focus on regulating the transaction).

101 See Brian Monroe, ATM Cards Tied to Virtual Worlds a “Money Launderer’s Dream,” MONEY LAUNDERING ALERT, Dec. 2007, available at https://www.world-check.com/media/d/content_pressarticle_reference/Rijock_Foretnt_20071120.pdf (showing an example of a potential money laundering operation that can happen over the Internet due to the lax regulations at the present time).
Consequently, as demonstrated by the two hypotheticals posited in this Comment, similar scenarios using different methods result in vastly different outcomes. There is far more room to maneuver for criminals when conducting money laundering operations over the Internet using virtual currencies. The very nature of the Internet makes it difficult for law enforcement to crack down on illegal activities, but that does not have to be the case.

Bitcoins epitomize the unregulated nature of Internet activities. Recent demand for Bitcoins by users around the world resulted in a dramatic increase in the price of Bitcoins, which was trading at an all-time high above $1,200 in November 2013. The ability of a Bitcoin user to use Bitcoins to accomplish a wide spectrum of tasks on the Internet, both legal and illegal, is a cause for concern. Additionally, the potential of the law to regulate the use of Bitcoins is limited due to the global and anonymous nature of the Internet. Consequently, it is more likely for legislators to extend the existing legal framework to cover such transactions, rather than create new legal

102 See, e.g., Straub, supra note 8, at 529 (advocating that statutory reforms and changes to the current regulatory scheme need to be made to account for the growth of virtual currencies in order for money laundering laws to remain effective).
103 See Solum, supra note 67, at 947 (advocating for the use of careful and targeted layer-approach to regulation of the Internet, where specific regulations only affect certain Internet activities and not others).
mechanisms.\textsuperscript{106} Even then, the ability of the government to regulate any aspect of Internet activity requires a fundamental rethink of the Internet’s base structure as an open-source platform.\textsuperscript{107}

E. The regulation of Bitcoin will result in the unavoidable sacrifice of privacy for financial transactions on the Internet and a push for a change in the way the Internet is viewed as an open-source network.

Bridging the gap between real world money laundering and virtual money laundering from a regulatory perspective requires a major leap concerning the structure of the Internet.\textsuperscript{108} The major problem that law enforcement


\textsuperscript{107} See, e.g., Jay P. Kesan and Andres A. Gallo, Optimizing Regulation of Electronic Commerce, 72 U. Cin. L. Rev. 1497, 1622 (2004) (concluding that in its current state, the Internet is too widespread and accessible globally for successful regulation to occur and that lack of clear enforcement hurts e-commerce).

\textsuperscript{108} See Thomas B. Nachbar, Paradox and Structure: Relying on Government Regulation to Preserve the Internet’s Unregulated Character, 85 MINN. L. REV. 215, 316-17 (2000) (arguing that proposed government regulations to extend governmental oversight over the Internet would limit the freedom of Internet users and would destroy the Internet’s value as a source for free exchange). But see Michael A. Geist, The Reality of Bytes: Regulating Economic Activity in the Age of the Internet, 73 WASH. L. REV. 521, 570 (1999) (postulating that Internet regulation is necessary to ensure unhindered economic activity on the Internet and that regulation should come from every aspect of government).
encounters with services such as MtGox is the anonymous nature of its user base.\textsuperscript{109} Without being required to verify their real identities and addresses, users can maintain a trading account on MtGox, where their activities are unregulated by the website.\textsuperscript{110}

Regulation of sites like MtGox would inevitably require that such sites maintain a record of their users’ personal information and a system of identification verification.\textsuperscript{111} However, such requirements would require the cooperation of multiple states and would create issues of privacy and information security.\textsuperscript{112} Consequently, in order for current anti-money laundering laws to be effective on the Internet, a degree of privacy will invariably have to be sacrificed.

\textbf{IV. RECTIFYING THE LEGAL PURGATORY OF VIRTUAL CURRENCIES WITHIN THE BANK SECRECY ACT}

Congress must take additional measures to curb the use of virtual currencies to launder money and bring regulation of those virtual currencies under the umbrella of

\textsuperscript{109} See, e.g., Bitcoin Wiki: MtGox, supra note 47 (stating that the underlying philosophy behind Bitcoin exchange revolves around anonymity).

\textsuperscript{110} Id. (stating that MtGox does not require personal information for a user to have an account on the website and to engage in trades).

\textsuperscript{111} See Solum, supra note 67, at 922 (arguing that digital identification verification is an easy solution for regulation of the Internet, which can be achieved securely, privately, and anonymously, with minimal breaches of privacy).

the BSA. Creating a level of parity between formal financial institutions and IVTS would foster similar levels of responsibility and awareness for illegal activities involving financial crimes.113 It would effectively close the loophole that currently exists for money launderers to use virtual currencies in laundering illegally acquired funds. To accomplish this, Congress must pass new updates to the BSA to address the new issues surrounding the advent of the Internet.114

A. The Bank Secrecy Act must be updated to classify Internet transactions as IVTS and virtual currencies as MSB in order to expand the purview of the BSA.

Under the existing definition of IVTS, virtual worlds on the Internet exist in a grey area where legal boundaries are nebulous.115 In order to rectify this problem, the government should update regulations to reflect the need for every IVTS to register with the Treasury Department.116 Once websites dealing with financial transactions of virtual currencies are officially

113 See Landman, supra note 97, at 5181 (postulating that once existing BSA regulations are expanded to cover virtual worlds, law enforcement and intelligence officials can begin cracking down on one of the last remaining unregulated methods for transferring terrorist funds).

114 See Rosette, supra note 96, at 301 (arguing that after the passage of the PATRIOT Act in the US, the FATF released a number of recommendations attempting to expand existing MSB regulations into more informal systems).

115 See, e.g., Money Laundering Prevention, supra note 3 (stating that FinCEN does not address virtual currencies or virtual transactions in their guidelines).

116 See 31 C.F.R. § 103.41 (2008) (requiring all classifiable MSBs to be registered with the FDIC, but because virtual currencies exist in a grey area, they do not have to register).
declared as IVTS, it will allow for greater reach from the BSA to close down money laundering loopholes.\footnote{Cf. Mayer-Schönberger & Crowley, supra note 32, at 1825-26 (making the argument for self-regulation on the Internet and that the government should not interfere in regulating activity on the Internet. The authors claim that this is the most effective way for the Internet to police itself, and no amount of government regulation can achieve similar results).} As part of the redefinition of legal frameworks regarding transactions over the Internet, the new regulations should expand the classifications of MSB to include services that convert between virtual currencies and real world currencies.\footnote{But see Nikolei M. Kaplanov, Note, Nerdy Money: Bitcoin, The Private Digital Currency, And The Case Against Its Regulation, 25 LOY. CONSUMER L. REV. 111, 169-171 (arguing against regulation of Bitcoins because prosecutors looking into financial crimes can use the P2P ledgers to investigate sources of irregularities).}

As it stands, the five classifications are not enough to categorize websites such as MtGox, but to expand the five classifications to explicitly address services that provide virtual currency transactions would directly incorporate such services under the regulations of the BSA. Once Congress expands existing BSA regulations to cover virtual worlds, prosecutors will have an easier time pressing charges against cyber-money launderers.\footnote{See Lormel, supra note 63 (advocating that MSB definition must be expanded in order for vulnerabilities and workarounds to be closed as the categories are too limited currently, allowing for terrorists and the like to exploit).}

\section*{B. Extend existing BSA regulations to cover Virtual IVTS.}

As soon as Congress updates the BSA to take into account the existence of virtual currencies and services that allow for conversion of virtual currencies into real world
money, these services are obligated to be subject to BSA regulations. To that end, these services must implement comprehensive anti-money laundering and financing programs, as stipulated by the BSA. That would ensure that these informal services follow the same rules as that of formal financial institutions. This expansion of regulation into virtual worlds will reduce criminal abuse of these systems and close loopholes.

Under existing regulations, institutions must: identify customers as they open accounts by obtaining information such as the customer’s name, address, date of birth, and taxpayer identification number; exercise reasonable efforts to verify the customer’s identity; maintain records and information obtained during the identification and verification process; and crosscheck with lists of individuals whose assets have been blocked or frozen. This would mean that websites like MtGox would no longer be able to enjoy the high level of anonymity that it does currently with its user base.

While this does pose some major issues over Internet privacy, that data does not need to be made public, but can be kept as a private record in the event that

120 See generally Bank Secrecy Act of 1970, supra note 7 (requiring informal value transfer systems to be treated in the same manner as formal institutions).
121 See FINCEN, BANK SECRECY ACT REQUIREMENTS (2007), http://www.fincen.gov/statutes_regs/guidance/pdf/bsa_quickrefguide.pdf, 1 (illustrating that once virtual currencies are deemed MSBs, a transactional trail can be created for all transactions, which will allow the BSA to govern).
122 See, e.g., Money Laundering Prevention, supra note 3 (recognizing that these regulations were created for formal financial institutions to ensure that any suspicious CTRs could be traced back to specific transactions and people).
123 See, e.g., Bitcoin Wiki: MtGox, supra note 47 (stating that the core premise of Bitcoins and Bitcoin traders such as MtGox revolves around anonymity).
investigations are necessary into specific users. This would be a similar procedure to when individuals open a bank account with any banking institution in the United States. Without this key requirement, it will remain near impossible for law enforcement to track down the identities and sources of those involved in virtual money laundering.\(^\text{124}\)

C. Existing regulations must be extended to recognize virtual currencies as legally being the same as real world currencies in order for any policies to be successful

Although to require virtual IVTS to maintain strict identification procedures would appear to be an extreme overreach of regulation, traditional banks implemented similar programs when shifting to online banking in the last ten years.\(^\text{125}\) A potential solution for websites and users who want to reduce the amount of personal information needed to register and use the virtual MSB is to create a dual classification account system. What that means is that there will be types of accounts, with differing levels of scrutiny. One type will permit users to engage in financial transactions and the other one will not. The former account


\(^\text{125}\) See FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT (last visited Feb. 10, 2014) http://www.ffiec.gov/pdf/authentication_guidance.pdf (outlining the authentication program that banks within the United States underwent in order to close loopholes in formal financial institutions).
will involve strict adherence to the BSA regulations regarding identification, while the latter account will not.\footnote{Id. (analyzing the technology used by the banking industry to authenticate identification).}

However, in order to impose any sort of drastic restructuring of the way business is done on the Internet through IVTS will invariably require the support and backing of the FATF.\footnote{See International Standards, supra note 5, at 7 (outlining that the FATF’s support is necessarily to ensure global uniformity with regards to new regulations over virtual currencies, as evidenced by the far reaching effects of the FATF recommendations on money laundering).} Criminals can easily circumvent any domestic regulations made by the United States to impose changes to the online IVTS system. Consequently, full FATF support is necessary to ensure uniform changes and relative parity of recommendations in how global governments treat the issue of virtual currencies as IVTS.\footnote{See generally Financial Action Task Force, supra note 5 (laying out the functions of the FATF as an inter-governmental body created to make and enforce policies regarding international money laundering).}

V. CONCLUSION

As the FBI has acknowledged, the new frontier of money laundering and financial crimes using the new medium of virtual currencies is a brutal reality. With the increasing virtualization of the world and the dramatic growth of virtual economies and currencies in the last decade, law enforcement officers currently lack the ability to prosecute financial criminals hiding in cyberspace due to lagging regulations not suited for the virtual world. Once relegated to the realm of academia, virtual currencies, such as Bitcoin, have become increasingly commonplace as a method of exchange on the Internet. The ability of Internet users to convert virtual currency into real currency
highlights the integration of the virtual economy into the real world.

In order to rectify that problem, lawmakers must be aware of the challenges faced by law enforcement in tracking down cybercriminals. The legal grey area of virtual worlds poses a specific problem and needs to be rectified in order for successful regulation to occur. As this Comment demonstrates, the use of virtual currencies to conduct illegal financial activities is not only a distinct possibility, but also a likely reality, given the ease with which users can escape regulation and law enforcement. Only when Congress declares virtual worlds and currencies to be IVTS can there be regulations on the vulnerabilities of these platforms. The Department of the Treasury should examine the possibility of classifying virtual worlds and economies as IVTS in order to subject these gaps to the BSA’s anti-money laundering regulations. Furthermore, users will have to sacrifice a certain degree of anonymity in order to allow for verification of user identities, similar to that of verification during the banking process.

A major leap from the government is required in order to bridge the gap between the 20th century and 21st century concerning financial crimes. The world will only become increasingly more dependent on the Internet and current regulations are insufficient in dealing with this new challenge. To stand idly by and allow the Internet to remain in a legal grey area concerning financial regulation is not only unreasonable, but also a threat to the foundations of the global economy.