

JOURNAL OF LAW AND CYBER WARFARE

- I. Counterterrorism Measures via Internet Intermediaries: A First Amendment & National Security Dilemma.....1
Mohamed H. Aziz
- II. Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks.....23
Elizabeth Mavropoulou
- III. Legal Implications of Vulnerability Disclosure in International Conflict.....93
Thomas Cross
- IV. Virtual Crimes, Actual Threats: Deterring National Security Offenses Committed Through Cyberspace.....108
Asaf Wiener

Editor-in-Chief

Daniel B. Garrie, *Partner, Law & Forensics*

Senior Associate Editors

Michael Mann
Samantha Tucker
Radhika Tiwari
Tarique Collins

Junior Associate Editors

Jennifer Chan
Barry Dynkin
Anthony Ford
Geoffrey Kalender
Zachary Levy
Mary Beth Winningham

Editorial Board

Christopher Burgess <i>Founder & CEO, Prevendra</i>	Robert Clark <i>Cyber Attorney, Army Cyber Institute</i>
Jean-Claude Knebelar <i>Consul General of Luxembourg to New York</i>	Robert Bair <i>Lieutenant Commander, United States Navy</i>
Jack Dever <i>Director, Business Intelligence Unit, General Electric</i>	Deborah Housen-Couriel <i>Special Counsel, Zeichner Ellman & Krause</i>
Dr. Larry Ponemon <i>Chairman, Ponemon Institute</i>	William Spernow <i>Chief of Security, Virus Inspector</i>
Jeremy Kroll <i>CEO, K2 Intelligence</i>	Eric Jensen <i>Law Professor, BYU</i>
John Dever <i>General Counsel of Defense Firm</i>	Uma Chandrashekhar <i>Global Information Security and Privacy Leader at Edwards Life Sciences</i>
Major Reserve, US Army	Vincent Scott <i>GBS-ITS Cybersecurity, Proctor & Gamble Company</i>
Dr. Joseph Weiss <i>Managing Partner, Applied Control Solutions</i>	Rhea Siers <i>Senior Associate at the GWU Cyber Security Initiative</i>
Shane Reeves <i>Associate Law Professor, US Military Academy, West Point</i>	Richard Borden <i>Chief Privacy Lawyer, Department of Trust and Clearing Corproartion</i>
Mitchell Silber <i>Executive Managing Director, K2 Intelligence</i>	Professor Michael Schmitt <i>Director, Stockton Study of International Law at the US Naval War College</i>
Noah Bledstein <i>IT Data Privacy Leader at GE Healthcare</i>	
Retired Major U.S. Airforce	

Legal Implications of Vulnerability Disclosure in International Conflict

Thomas Cross*

INTRODUCTION

Actors who attack computer systems often seek to accumulate knowledge of computer security vulnerabilities they can leverage in launching those attacks. Exclusive knowledge of security vulnerabilities in the software systems of one's adversaries can convey an offensive advantage to an attacker. However, every time a vulnerability is exploited in an attack, a risk exists that the victim will learn the vulnerability exists, and how to exploit it. The victim may use that information to protect themselves, but they may also use it to launch their own attacks against the initial aggressor, or other targets. Widespread attacks launched on the Internet

* Tom Cross is the CTO of Drawbridge Networks, where he is creating next generation enterprise security technologies. He is credited with discovering a number of critical security vulnerabilities in enterprise class software and has written papers on collateral damage in cyber conflict, vulnerability disclosure ethics, security issues in Internet routers, securing wireless LANs, and protecting Wikipedia from vandalism. Tom was previously Director of Security Research at Lancope, where he worked on network anomaly detection with Netflow, and Manager of the IBM Internet Security Systems X-Force Advanced Research team, where he focused on advancing the state of the art in network intrusion prevention. He has a Bachelor of Science in Computer Engineering from the Georgia Institute of Technology. All views expressed in this paper are his own.

have the foreseeable consequence of conveying vulnerability information to a large number of people, who may repurpose that information in a variety of ways.

The Law of Armed Conflict requires combatants to choose means and methods of warfare that avoid or minimize incidental harm to civilians. This obligation applies to indirect and direct collateral damage. This paper assesses the question of whether attacks that broadly disseminate vulnerability information may violate the Law of Armed Conflict because, those vulnerabilities could be reused in attacks that impact civilians or civilian infrastructure.

The paper begins by providing some background on security vulnerability disclosure and the repurposing of vulnerability information. Part II discusses a real world example: the repurposing of a vulnerability disclosed due to the Stuxnet malware. Part III discusses how indiscriminate attacks are treated under the Law of Armed Conflict and how this treatment might be applied to the context of broadly disseminated vulnerability information. The final section provides a conclusion and some follow-on questions.

I. MALICIOUS REUSE OF VULNERABILITY INFORMATION

Successful attacks against computer systems often involve the exploitation of computer software vulnerabilities – flaws in computer software that an attacker can leverage to gain control of a computer system or otherwise impact the confidentiality, integrity, and availability of the data and services on

that system.¹ Ideally, vulnerabilities in computer software are discovered during the development and testing of that software by the organization responsible for maintaining it. However, some vulnerabilities are missed by software developers, and are later discovered by independent third parties after the software is already in use on computer networks. In addition, malicious actors have also been known to intentionally induce vulnerabilities into software that they seek to target.

Many third parties who discover security vulnerabilities have no desire to see them used in attacks. Typically, third parties communicate the vulnerability details to the responsible software vendor, who then prepares an update that fixes the problem. Public disclosure of a software vulnerability before the vendor has the opportunity to prepare an update can result in attack activity that victims are unprepared to defend themselves against.² Therefore, many independent security vulnerability researchers choose to engage in a coordinated vulnerability disclosure process with software vendors, in which information about the vulnerability is kept secret until an update that fixes

¹ See *Definition of a Security Vulnerability*, MICROSOFT, <http://msdn.microsoft.com/en-us/library/cc751383.aspx> (last visited Feb. 2, 2015).

² Applying updates that fix vulnerabilities in software is the primary step that computer users take to protect themselves against attacks that target those vulnerabilities. Obviously, if no update is available, then this is impossible. Users also employ Network Intrusion Prevention Systems to detect and block attacks that target vulnerabilities, but if a particular vulnerability has not been publicly disclosed and there is no update available that fixes it, Network Intrusion Prevention Systems may also lack the necessary logic needed to detect attacks that target that particular vulnerability.

the problem is available. When the update is released, both the vendor and the researcher publicly disclose the existence of the vulnerability along with information about how to obtain the update that fixes it.³ In order to encourage this sort of coordinated disclosure, some software vendors offer to pay rewards or bounties to independent researchers who disclose vulnerabilities to them.

Sometimes, information about vulnerabilities falls into the hands of third parties who do wish to launch attacks. Actors who attack computer systems may seek to accumulate knowledge about software vulnerabilities that have not been reported to the vendor and are not fixed in an update.⁴ Exclusive knowledge of these vulnerabilities conveys an offensive advantage to the attacker, as those vulnerabilities can be leveraged to launch attacks that may be hard for victims to defend against.⁵ Often, malicious third parties employ reverse engineering to discover vulnerabilities in the software systems that they seek to target, but in some cases third parties have been known to directly induce vulnerabilities through covert action against the software developer.

³ See *Security TechCenter: Coordinated Vulnerability Disclosure*, MICROSOFT, <http://technet.microsoft.com/en-us/security/dn467923.aspx> (last visited Feb. 2, 2015).

⁴ See Kim Zetter, *U.S. Gov Insists It Doesn't Stockpile Zero-Day Exploits to Hack Enemies*, WIRED (Nov. 17, 2014), <http://www.wired.com/2014/11/michael-daniel-no-zero-day-stockpile/>; see also Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, WHITEHOUSE BLOG (Apr. 28, 2014), <http://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities>.

⁵ See *supra* note 2.

In most circumstances, launching an attack that targets a software vulnerability involves taking the risk that the victim will learn about the vulnerability. Computer software vulnerabilities are usually exploited by sending input to the software that triggers the vulnerability. That input, known as an exploit, could come in a number of different forms, such as a specially crafted network packet, or a web page, or a word processor document sent as an email attachment.⁶ As the attacker must send the exploit to the victim's computer, the victim could capture it in transit. Forensic network packet capture technologies, record all transactions occurring over a network, and are often used for the purpose of recording attacks.⁷ Exploits that trigger security vulnerabilities are also frequently embedded into software that attackers install on the victim's computers. The details of these vulnerabilities may be unearthed by forensic investigators working on behalf of the victims to study the artifacts of the attack.⁸

Victims who become aware of a computer software vulnerability because it was used against

⁶ See *Malware Protection Center: The Exploit Malware Family*, MICROSOFT, <http://www.microsoft.com/security/portal/mmpc/threat/exploits.aspx> (last visited Feb. 2, 2015); see also *Exploit (computer security)*, WIKIPEDIA, [https://en.wikipedia.org/w/index.php?title=Exploit_\(computer_security\)&oldid=631804551](https://en.wikipedia.org/w/index.php?title=Exploit_(computer_security)&oldid=631804551) (Last modified Oct. 30, 2014).

⁷ See Joe Habib, *Network Forensics and Digital Time Travel* (Nov. 16, 2009), TECHNEWSWORLD, <http://www.technewsworld.com/story/exploits-vulnerabilities/68651.html>.

⁸ See Brian Krebs, *Experts Warn of New Windows Shortcut Flaw* (Jul. 10, 2010), KREBS ON SECURITY, <http://krebsonsecurity.com/2010/07/experts-warn-of-new-windows-shortcut-flaw/>.

them by an attacker, have the option of leveraging that vulnerability to launch their own attacks, either against networks operated by the original attacker, or against third parties. The original attacker may not be aware that the victim has discovered the details of the vulnerability, and they may not be prepared to defend their own networks against such attacks.⁹

Even when the victim does not wish to launch attacks, they may feel pressure to immediately disclose information to the public about a vulnerability, without waiting for the software vendor to prepare an update first.¹⁰ Hypothetically, this would inform other potential victims of the attack activity, so that they can take immediate defensive measures while they wait for an update. However, the ability of different computer users to protect themselves against attacks that target vulnerabilities, that haven't been fixed in an update, varies widely. For this reason, there are many threat actors who seek to take advantage of opportunities to target vulnerabilities that have not yet been fixed by software vendors, and public disclosure of an unrepaired vulnerability that has been used in targeted attacks can result in a large amount of

⁹ Although the original attacker is aware of the vulnerability, if they are using it offensively they may not have developed defensive measures to protect against attacks that target it, or those defensive measure may have only been deployed in a limited fashion in order to protect the secrecy of the vulnerability. Because the vulnerability is not publicly disclosed, no update would be available that patches it, and so most networks (e.g. civilian networks) would be unprotected.

¹⁰ See Holly Stewart & Tom Cross, *Lessons Learned: Can Alerting the Public About Exploitation Do More Harm Than Good?*, VIRUS BULL. CONF. 58–59 (2013), <https://www.virusbtn.com/files/StewartCross-VB2013.pdf>.

follow-on attack activity.¹¹ If victims wait until a vendor update is available before public disclosure, this can help minimize the amount of harm, but victims will not always make that choice.

II. STUXNET: AN EXAMPLE OF MALICIOUS VULNERABILITY REUSE

Stuxnet is a perfect example of a state sponsored attack that resulted in broad dissemination of vulnerability information. Stuxnet was a self-reproducing Internet worm that spread automatically throughout the Internet using several security vulnerabilities in Microsoft Windows that Microsoft was unaware of at the time and for which there was no update. Although Stuxnet's destructive payload only executed on specifically targeted hosts, the malware itself infected thousands of computer systems worldwide and distributed vulnerability information to each one. Eventually Stuxnet was discovered on a victim's computer, and analyzed by their anti-virus software vendor. In an attempt to alert the public about the security threat posed by Stuxnet, that anti-virus software vendor publicly disclosed one of the vulnerabilities that Stuxnet targeted before Microsoft was able to release an update. During the period of time between public disclosure of that vulnerability and availability of the update from Microsoft that fixed it, a number of different threat actors jumped on the bandwagon, using the vulnerability to propagate a variety of different kinds of malware. The most successful of these was the Salty malware gang.¹² Salty has been used to steal

¹¹ See generally *id.*

¹² See *id.* at 65–66.

financial information from personal computers, relay spam, break into web servers, and crack encrypted passwords.¹³

The creators of Stuxnet bear some level of responsibility for the follow-on attack activity that occurred as a result of the premature public disclosure of one of the vulnerabilities that Stuxnet exploited. Instead of using that vulnerability to launch an attack, the creators of Stuxnet had the option of disclosing it to Microsoft so that Microsoft could prepare an update. The use of the vulnerability could also have been limited to targeted attacks, in order to minimize the risk that the vulnerability information might fall into the wrong hands. However, they chose instead to embed the exploit for the vulnerability into a self reproducing computer program that subsequently infected computer systems all around the world,¹⁴ thus maximizing the exposure of the vulnerability information and leading, indirectly, to widespread attacks on computer systems by a collection of financially motivated criminal gangs. In doing so, did the creators of Stuxnet violate the Law of Armed Conflict?

III. VULNERABILITY INFORMATION AND THE LAW OF ARMED CONFLICT

¹³ See Nicolas Falliere, *Sality: Story of a Peer-to-Peer Viral Network*, SYMANTEC 6 (2011), http://www.symantec.com/connect/sites/default/files/sality_peer_to_peer_viral_network.pdf.

¹⁴ See Jarrad Shearer, *Symantec Security Response: W32.Stuxnet*, SYMANTEC http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99 (Last modified Feb. 26, 2013).

The *Tallinn Manual on the International Law Applicable to Cyber Warfare* is the best available interpretation of the Law of Armed Conflict as it applies to cyber war. The *Tallinn Manual* provides three rules that might apply to the use of cyber weapons that broadly disseminate vulnerability information. Rule 43 prohibits indiscriminate means and methods of launching attacks.¹⁵ Rule 51 prohibits any excessive civilian harm in relation to the military advantage anticipated by a particular operation.¹⁶ Rule 54 requires attackers to take all feasible precautions in the choice of means or methods of warfare to avoid or minimize incidental injury to civilians, loss of civilian life, and damage to, or destruction of, civilian objects.¹⁷ Let us consider the impact of each rule on vulnerability disclosures that occur as a consequence of cyber attacks, with particular reference to the real world example of Stuxnet.

It has been argued that Stuxnet did not directly violate Rule 43 of the *Tallinn Manual* because its payload delivery was highly targeted.¹⁸ Rule 43 is only implicated by means or methods of attack that can cause indiscriminate injury or death to people, or that can damage or destroy physical objects.¹⁹ Although Stuxnet infected computer systems indiscriminately, its harmful payload, which

¹⁵ See MICHAEL N. SCHMITT, *TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE* 121 (3rd ed. 2013).

¹⁶ See *id.* at 132.

¹⁷ See *id.* at 140.

¹⁸ See Robert Fanelli & Greg Conti, *A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict*, INT'L CONF. ON CYBER CONFLICT 329–330 (2012).

¹⁹ See *supra* note 15, cmt. 5 at 122.

was allegedly designed to destroy a uranium centrifuge located in Iran, was only executed in specific, targeted circumstances.²⁰

Likewise, none of the malware subsequently propagated by third parties using the vulnerabilities disclosed as a consequence of Stuxnet was capable of causing injury or death to people, nor was any of it capable of permanently damaging or destroying physical objects. However, it is useful to consider the implications of a scenario in which a vulnerability revealed by broadly disseminated malware like Stuxnet was used in such a fashion. When vulnerability information is reused maliciously in peacetime, it is typically in the context of financially motivated attack activity. However, in a time of war, the reuse of broadly disseminated vulnerability information in attacks that harm people and physical objects may be foreseeable. For example, consider the consequences of publicly disclosing an unpatched vulnerability in a piece of vital medical equipment in the midst of an armed conflict.

If an actor launches an attack that has the consequence of broadly disseminating information about a software vulnerability, this could set off a foreseeable chain of events in which that vulnerability information gets reused by third parties in follow-on attacks that might harm civilians or civilian infrastructure. The *Tallinn Manual*, Lit. (b) of Rule 43:

[A]ddresses cyber means and methods that . . . have effects that cannot be limited in any circumstances. The crux of *lit. (b)* is a prohibition on weapons that by their nature generate effects that are incapable

²⁰ See *supra* note 17.

of being controlled In particular, *lit.* (b) encompasses cyber weapons that create an uncontrollable chain of events.²¹

It may be tempting to consider vulnerability reuse to be the sort of “uncontrollable chain of events” that Rule 43 is intended to sanction, but there are strong arguments against doing so. A cyber weapon can be conceived of as a system with multiple components, including exploits for vulnerabilities, propagation code, command and control capabilities, a payload designed to deliver damage to a target, and other components. Each actor has a choice regarding what sort of attack payload to associate with a particular propagation method when they create a cyber weapon. Rule 43 speaks to both the potential consequences of that payload, as well as how the weapon is targeted. Therefore, it makes sense to read Rule 43 as applying to a particular weapon as a whole, including how its propagation methods and payload work together, in the context of how a particular actor employed it, instead of considering how individual components of a particular weapon might be picked up and repurposed differently by other actors.

If Rule 43 were interpreted as applying to potential reuse of every component of a weapon individually, this would have the consequence of holding the creators of cyber weapons to a higher standard than other actors who engaged in behavior with similar consequences. For example, during a time of war, a vulnerability that was publicly disclosed on an email mailing list might foreseeably

²¹ See *supra* note 15, cmt. 4, at 121.

be reused as a component of a weapon capable of harming people or physical objects. However, Rule 43 would not apply to the act of disclosing that vulnerability through a mailing list, because an email is not a “means or method of warfare.”

The sort of damage to civilian infrastructure caused by secondary attacks resulting from a vulnerability disclosure could factor into the proportionality analysis required by Rule 51, which prohibits harm that is excessive in light of the military advantage anticipated by an operation. The *Tallinn Manual* makes it clear that Rule 51 applies to *indirect* collateral damage,²² so it may apply to a scenario where vulnerability disclosure foreseeably results in attack activity by third parties that is harmful to civilians, if the damage likely to be caused by those attacks meets the threshold for consideration. The *Tallinn Manual* states that damage to data alone may not qualify,²³ so the sort of financially motivated attack activity likely to occur in peacetime as a result of a vulnerability disclosure may not meet that threshold. In the case of Stuxnet, the damage caused by third party attackers likely did not meet the threshold. However, in a time of war, more significant third party attacks might be foreseeable.

Rule 54 can also be applied to a scenario in which actors are contemplating an attack that might result in vulnerability disclosure. Rule 54 requires “those who plan or decide upon a cyber attack” to take “all feasible precautions in the choice of means or methods of warfare employed in such an attack, with a view to avoiding, and in any event, to

²² See *id.*, cmt. 6, at 133.

²³ See *id.*, cmt. 5, at 108.

minimizing, incidental injury to civilians, loss of civilian life, and damage to or destruction of civilian objects.”²⁴ The *Tallinn Manual* makes it clear that Rule 54 also applies to *indirect* collateral damage.²⁵ Notably, Rule 54 does not strictly prohibit all attacks that have indirect collateral effects. The *Tallinn Manual* clarifies that although attackers do have an “obligation to consider alternative weapons or tactics to minimize collateral damage . . .” they “need not select alternative weapons or tactics that will yield less military advantage . . .”²⁶

In the context of Stuxnet, it may be worth asking whether it was possible to achieve the same military objective without disseminating the malware so broadly. Stuxnet infections were discovered on computer systems all over the world.²⁷ However, the alleged target was in a very specific geographic region. There are a variety of different command and control techniques that hypothetically could have been employed to limit the spread of Stuxnet to a smaller population of hosts.²⁸ Whether these techniques were practical to employ in this case is difficult to assess, but had the consequences of the follow-on attack activity been greater, this question may have attracted deeper scrutiny.²⁹

²⁴ See *id.* at 140.

²⁵ See *id.*, cmt. 5, at 140.

²⁶ See *id.*, cmt. 2 & 3, at 140.

²⁷ See *supra* note 14.

²⁸ See generally David Raymond, et al., *A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons*, INTERN’L CONF. ON CYBER CONFLICT (2013).

²⁹ It is possible to hide payload information (including vulnerability details) intended for specific targets within a widely disseminated malware by encrypting that information with a key that is based on characteristics of the targets that are difficult to guess or determine independently. This

IV. CONCLUSION

Actors planning attacks involving cyber weapons have an obligation to take into consideration the dissemination of vulnerability information that might result from their attacks. The broad or indiscriminate dissemination of a cyber weapon that exploits an as yet unknown and undisclosed computer security vulnerability may violate the Law of Armed Conflict, if there is a foreseeable possibility those vulnerabilities could be reused in attacks that harm civilians or civilian infrastructure, and alternative, less destructive means of obtaining the same military objectives are available, or the amount of foreseeable harm is excessive relative to the anticipated military advantage gained as a consequence of the operation.

Actors should look for ways to limit the dissemination of vulnerability information as much as possible without compromising their military objectives, not just to protect their own proprietary knowledge of those vulnerabilities, but also to protect civilians from their malicious appropriation by others. This obligation is particularly high in a time of conflict, when vulnerabilities might foreseeably be appropriated in attacks that have the potential to cause significant harm. Further investigation of these issues would benefit from information about how the proliferation of weapons and weapon technologies has been treated under the Law of Armed Conflict in the past, as that treatment

approach could be used to limit the vulnerability information disseminated by a cyber attack. However, it can't prevent analysts from learning the details of vulnerabilities that are used indiscriminately.

may be relevant to the proliferation of vulnerability information and other cyber capabilities.

Acknowledgements: The author would like to thank Greg Conti for a thoughtful review of the paper.

