2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict

Robert Fanelli
United States Cyber Command
Fort Meade, Maryland, USA

Gregory Conti
United States Military Academy
West Point, New York, USA

Abstract: Throughout history, the law of warfare has evolved to protect non-combatants and limit collateral damage. The same legal and ethical constraints apply to the conduct of cyber warfare, where it is similarly desirable to limit the effects of offensive actions to specific locations and groups. However, conventional wisdom suggests that this is extremely difficult, if not impossible to accomplish in the cyber domain. In this paper, we argue to the contrary. It is possible to constrain the effects of cyber actions to specifically desired, legitimate targets while significantly limiting collateral damage and injury to non-combatants. To this end we present a generalized methodology for analysis of the targeting and effects of cyber operations with respect to principles of lawful conduct in armed conflict. This methodology includes a framework of effects categories, target attributes and control measures to direct and constrain cyber operations. It also includes a process for evaluating these effects and controls against the principles for lawful conduct in armed conflict. We illustrate the methodology in action by applying it to W32.Stuxnet, software widely considered to be a cyber weapon. Our results indicate that it is entirely possible to analyze complex cyber war problems, identify legally authorized courses of action, and focus effects on desired targets while greatly minimizing collateral damage.

Keywords: *cyber operations, targeting, collateral damage, law of armed conflict*

1. INTRODUCTION

While unfortunate, armed conflict has existed since the dawn of man. Over time, customs, agreements and laws have evolved to define what actions are permissible and prohibited in armed conflict. For example, among other requirements, humanitarian law imposes a duty on combatants to avoid injury to non-combatants and to limit collateral damage [1]. In general,

The views expressed in this article are those of the authors and do not reflect the official policy or position of the US Cyber Command, United States Military Academy, Department of the Army, Department of Defense, or United States Government. All information and sources for this paper were drawn from unclassified material.

standards for behavior in armed conflict on land, at sea or in the air are well-understood, having evolved over many years.

A similar understanding for warfare in the cyber domain does not yet exist. Much work has examined the legal aspects of operations in the cyber domain, attempting to reconcile such operations with existing notions of what constitutes armed conflict or an act of war [2,3,4]. However, the literature is mostly silent on how we may actually execute cyber operations in a manner that complies with accepted standards for conduct in armed conflict in particular. Some believe that constraining the effects of cyber operations is technically infeasible given the complexity and interconnectedness of information systems and networks, making all such operations illegal [5]. We argue that it is indeed possible to comprehensively study the operational factors and conduct cyber operations within legal and ethical constraints while achieving legitimate military objectives.

In this paper we make several contributions. We introduce a methodology to categorize the effects of cyber operations. We also present a framework of target attributes and control measures to direct and constrain cyber operations. Finally, we present a general methodology for evaluating these effects and controls against the principles for lawful conduct in armed conflict.

This paper is organized as follows. Section 2 places our research in the field of related work. Section 3 presents our generalized methodology. Section 4 examines application of the methodology to a cyber operation. Section 5 presents our conclusions and promising directions for future work.

2. BACKGROUND AND RELATED WORK

There is a great deal of interest in the opportunities and challenges of conducting military operations in cyberspace. A number of definitions exist in the literature for the term 'cyberspace.' For this work, the definition proposed by Daniel Keuhl is suitable: "…cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies." [6]

A commonly held view of cyberspace is one limited to computer systems connected by the TCP/IP-based Internet. However, Keuhl's definition of cyberspace includes a larger set of systems, protocols, architectures and functions including, but not limited to, those found on the Internet. Thus it is important that our discussion is sufficiently general, and our results are sufficiently flexible, to address the full range of information systems, networks and transmission media in cyberspace. Still, the framework must retain sufficient specificity to inform actual offensive action in the domain.

The United States Department of Defense and others have only recently recognized cyberspace as a separate domain of armed conflict besides land, sea, air and space [7]. Despite being a

distinct domain with unique qualities, the cyber domain requires standards for lawful behavior in armed conflict just as do the other domains [1]. Despite progress, we have not yet fully determined how the customs and body of law that define acceptable behavior in armed conflict will apply to the cyber domain.

Several authors have attempted to relate concepts of strategic warfare and deterrence to the cyber domain. [8,9,10] However, these works do not address nature of offensive action in the domain at the operational and technical levels.

A number of authors have also discussed legal aspects of cyber operations. Much that has emerged from this discussion, such as the 'Schmitt Criteria' [4], is concerned with the role of cyber operations in terms of *jus ad bellum*, or determining when resorting to war is justified and what constitutes an act of war.

One point of debate is whether or not cyber operations can, in fact, constitute armed conflict. Sklerov proposes "an effects-based approach, sometimes called a consequence-based approach, in which the attack's similarity to a kinetic attack is irrelevant and the focus shifts to the overall effect that the cyber attack has on a victim state." [2] Cyber operations do in fact amount to armed conflict when their effects are consistent with those of more established, kinetic forms of armed conflict, highlighting the need to pay particular attention to the potential effects of cyber operations.

For this work, we set aside the concerns of *jus ad bellum* and focus instead on *jus in bello*, the rules for lawful conduct of armed conflict *after* the decision to resort to military action is made. *Jus in bello* imposes duties to use restraint in the application of force, minimize suffering, and distinguish between legitimate military targets and non-combatants when conducting attacks. Further, combatants have a duty to control the collateral damage that may result from military operations. [1,3]

Sklerov identifies four principles of *jus in bello*:

1. Distinction: combatants have a duty to ensure attacks are directed at legitimate military objectives and to minimize collateral damage.
2. Necessity: the application of force must be limited to only the amount necessary to accomplish a valid military objective.
3. Humanity: weapons designed to cause unnecessary suffering are prohibited.
4. Proportionality: limits the use of force to situations in which the expected military advantage outweighs the expected collateral damage to civilians and their property. This does not require avoiding all collateral damage; rather, such damage must not be out of proportion with military necessity [2].

In addition to these principles, Schmitt cites a principle of *discrimination* [1]. This prohibits the use of 'indiscriminant' weapons or tactics, those incapable of avoiding damage to non-combatants.

These well-established principles dictate that one must be able to precisely target and control the effects of the weapons and techniques employed in armed conflict. Beyond having sufficient control, one must also ensure operations target valid military objectives in accordance with the *jus in bello* principles. "Those who plan or decide on attack have an affirmative duty to 'do everything feasible' to verify that intended targets are legitimate." [1]

For this work, we shall focus on the principles of discrimination, distinction and proportionality. Methods for ensuring cyber operations adhere to these three principles differ most from those for kinetic operations, posing the most significant challenges. The principles of necessity and humanity are similar in both kinetic and cyber operations. Compliance will follow from meeting the challenges posed by the other three principles.

The methods to discriminate between combatant and non-combatant and to reduce collateral damage in the kinetic domains of land, sea, air and space are relatively well understood. The effects of actions in the kinetic domains tend to be well localized in physical space. Similarly, physical science and modeling provide accurate predictions about the duration and spread of such effects. Admittedly, achieving these goals in practice is not always easy, mostly due to 'fog of war' and limited intelligence about the true nature of a target.

In the cyber domain, measures of location, distance and time may be less effective for ensuring compliance with the principles of *jus in bello* than they are in the physical domains. We also have far less history and experience dealing with the questions of how to target and constrain effects in the cyber domain. However, the requirement to conduct cyber operations in a manner consistent with *jus in bello* remains. Thus there is the need for a methodology, such as that presented here, to analyze cyber operations effects, targeting and control measures in terms of the lawful application of force in armed conflict.

3. A METHODOLOGY FOR CYBER OPERATIONS TARGETING AND CONTROL

'Cyber weapons,' and those wielding them, must be capable of operating in accordance with the principles of *jus in bello*. This entails the capability to direct effects at valid military targets using controlled amounts of force and to minimize collateral damage. Organizations conducting cyber operations require sufficient intelligence capabilities for accurate targeting plus agile and robust command processes to control and to accurately assess their effects. With respect to tools, these requirements differentiate cyber weapons from the more general category of malicious software, or malware. Malware is frequently indiscriminant and poorly controlled, seeking to spread and cause effects as widely as possible with little regard for the nature of the victims. The methodology presented here seeks to provide a framework in which those from the technical, legal and policy making disciplines can achieve consensus on lawful conduct for specific cyber operations and weapons.

A. Cyber Operations Effects

The potential severity and scope of a cyber weapon or operation's effects dictate the degree of control needed to act in accordance with *jus in bello* principles. Operations and weapons

capable of causing more severe damage, or with consequences more widespread in space and time, call for greater precision in targeting and control of effects. Thus we must have means to categorize the severity and persistence of effects. We define three categories of severity for effects:

Primary effects have the potential of directly affecting physical assets and human lives. This would include manipulating control systems to cause the malfunction of machinery, power outages, explosions, flooding, vehicle accidents or other physical destruction. It also includes rendering information systems and other electronics inoperative at the hardware and firmware level.

Secondary effects degrade or disrupt physical assets as a second-order consequence of effects in the cyber domain. Although a secondary effect does not have the immediate potential for direct physical destruction, it is still expected to affect physical assets. The disruption of information systems and networks in the cyber domain can affect physical assets reliant on them for control, monitoring and communications. Examples would include spoofing air defense systems, disabling telecommunication systems, incapacitating control systems for transportation or logistical networks, corrupting databases and manipulation of financial systems.

Indirect effects remain within the cyber domain, having only an informational impact. Attacks with indirect effects primarily impact human cognition and would be expected to affect the physical domain only through humans acting on the information perceived. Cyber operations having indirect effects would include military deception operations, delivering targeted messages to a populace and blocking or altering an adversary's messages.

A cyber weapon or operation may have the potential for causing multiple effects, possibly causing differing combinations of primary, secondary and indirect effects on different targets. We must consider each likely combination of target and effect for compliance with *jus in bello* principles.

We also define three degrees of persistence for effects:

Permanent. This level of persistence includes effects that require replacing hardware or extensive, time-consuming repairs. It also includes destruction of primary data and backups such that timely restoration is infeasible. Such effects would include disabling hardware through destruction of firmware, destruction of electronics through overloads, physical destruction of infrastructure or other property and loss of life.

Temporary. Temporary effects also persist after the operation ends; however, unlike permanent effects, recovery here entails actions of lesser cost in resources and time. Such procedures would fall within the scope of typical disaster recovery plans [11]. Examples include restarting disrupted telecommunications or electrical infrastructure, reloading operating systems and restoring data from backup media.

Transient. Transient effects abate quickly after the attack ends, with little effort on the part of the targeted entity. At most, recovery might include resetting or rebooting equipment. For

example, denial-of-service and traffic redirection attacks typically generate transient effects.

B. Target Attributes and Control Features

Cyber weapons and operations must have sufficient precision to ensure effects reach the intended targets while avoiding noncombatants. We require a flexible means to describe targets for the purpose of directing and constraining effects. We define three *target attributes* for cyber operations. Taken together, these attributes allow us to answer the questions: "Where is it?", "What is it?" and "Whose is it?" for a given target.

Geography. This attribute addresses the physical location of the target. This may be pertinent for two reasons. First, physical location within a given region, such as a national border, may define what is and is not a legitimate party to a conflict. Second, physical location may contribute to establishing a positive identification of the target, especially in ensuring it is not an entity with protected status and thus off-limits to attack. A geographic attribute may be as specific as a building, military installation or industrial facility or as broad as a nation or a military theatre of operations. The dynamic nature of networks and mobile devices may, in some circumstances, make determination of physical location difficult.

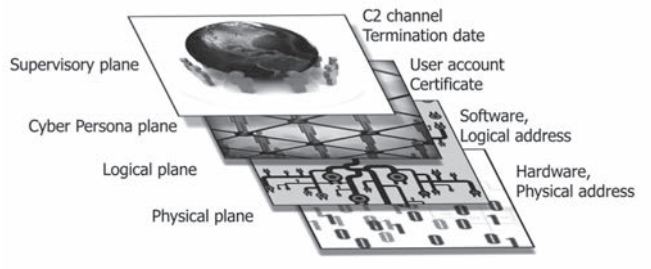
Function. This attribute addresses the purpose or current activity of a target. Identifying function provides a useful means to differentiate a legitimate target from other, nearly identical systems. For example, an industrial controller of a given type might be used for a humanitarian purpose in one location and a purely military role, such as producing munitions, in another. Further, combatants and protected entities could be intermingled on a shared network, in a cloud infrastructure or, through virtualization, on a single host. The information systems and networks that comprise cyberspace, by their flexible nature, may be the epitome of dual-use objects, potentially serving both civilian and military purposes [1]. A change of software or configuration could allow an information system to rapidly change function between civilian and military purposes. Thus, identification of a device's function may facilitate distinguishing intended, legitimate targets from others using similar hardware or software.

Persona. This attribute addresses the ownership and users of target. A persona attribute could relate to a person, business, government or other group. The personas involved with a given system or network may assist in identifying the intended target and separating legitimate targets from others. A persona may also be the primary descriptor for a target, indicating a person or group to be engaged wherever found in cyberspace, with less emphasis on geography and function.

After identifying the target in terms of geography, function and persona attributes, we must determine the specific information and technical features necessary for effective targeting and control of effects. The objective is to derive a set of *control features* sufficient to direct the effects to the intended target while avoiding disproportionate collateral damage or other unlawful consequences. Control features are specific values that a cyber weapon or operation can use to determine if effects should be delivered to a potential target device. The control features must be sufficiently general to encompass not only the TCP/IP based features frequently discussed in 'computer network attack' [12] but also the larger set of features available in the

array of devices and networks implied in the definition of the cyber domain. We divide the control features into four *planes*.

FIGURE 1. EXAMPLE CONTROL FEATURES BY PLANE



Physical Plane. The physical plane includes features of a device's hardware, its operating characteristics and its physical environment. Information about a device's hardware may identify its general type, its manufacturer or specific model, or possibly device unique identification by distinctive values such as embedded serial numbers.

Some devices, such as 'smart phones,' may provide direct information about their geographic locations through Global Positioning System or mobile network location services. Other physical features, such as clock settings, power sources and keyboard layouts may permit inferences to be drawn about the location of a device.

Physical features may provide information about the function of a device. Patterns of utilization, workloads, transmit and receive frequencies, function-specific firmware or environmental conditions may indicate a device's function and help differentiate it from similar devices. Similarly, the physical characteristics of devices attached to industrial control systems may provide information about the function or even the specific identity of the system.

Physical features that uniquely identify a device provide the potential for extremely precise targeting and control. Such information could tie the device to its owner or other persona and may also facilitate determining its function. Examples include serial numbers of hardware installed in computer systems or the International Mobile Equipment Identifier (IMEI) of a mobile device. Similarly, network address information associated with hardware on a persistent, if not permanent, basis can also provide device identification. Such features include medium access control (MAC) addresses for network interfaces, Mobile Identification Numbers (MIN) and International Mobile Subscriber Identity (IMSI) values on SIM cards.

Logical Plane. The logical plane includes features of the software on a device plus the configuration and state of that software. Primary examples are logical network addresses, such as Internet Protocol (IP) addresses. Although an IP address itself does not contain location information, the nature of IP networks and knowledge of address range assignments often make it possible to determine geographic location or ownership [13]. Other configuration items, such as time zone or language settings, may also help to infer a device's location.

Logical control features may also facilitate identifying the function of a device. The operating system and application software present, the configuration and state of the software and the data files, log files and other content stored on a device may differentiate devices having common hardware but serving different functions. Similarly, the programming of an industrial control system can provide useful information about the function of the system and possibly indicate its location and ownership.

Cyber Persona Plane. Cyber personas are identities in the cyber domain. These features are useful in determining the ownership, affiliation and users of a device. Physical personas and cyber personas often exist in one-to-many or many-to-many relationships. A person may have multiple cyber personas while a single cyber persona may in fact represent multiple, loosely related persons. An example of the latter case is the group 'Anonymous' [14].

The primary cyber persona control features are the user accounts on a device. These may include accounts for local and remote systems plus network services such as electronic mail. Cyber persona control features also include digital certificates, software license registration entries and stored biometric data. It may even be possible to capture images and audio from embedded cameras and microphones to definitively identify the user of a device.

Supervisory Plane. The supervisory plane contains the command and control features available to start, stop and redirect a cyber weapon or operation. This includes features related to human-in-the-loop command and control of targeting and effects during the operation. It also includes predefined trigger events for starting, stopping or changing some aspect of an operation and controls on the ability of cyber weapons to propagate autonomously.

This plane also includes temporal specifications for the timing and duration of effects. These may be specific start and stop times for operations or a duration limit for effects initiated in response to a trigger event.

C. Methodology for Enumeration and Analysis

Using the framework of effects, target attributes and control features presented above, we may now determine if a given cyber weapon or operation complies with *jus in bello* principles. This methodology involves considering the probable consequences of the operation against its precision in targeting and control.

First, we enumerate the likely primary, secondary and indirect effects of the cyber weapon or operation, along with the degree of persistence for each, on an *effects tableau*. In particular, any significant potential to cause death, bodily injury or destruction of property must be examined. Table I depicts an effects tableau with example entries.

After we have enumerated the likely effects of the cyber weapon or operation, we must examine its control features. This evaluation facilitates the military commander's determination if a planned operation complies with *jus in bello* principles. Alternatively, such analysis could be used during development to identify control features needed to ensure the cyber weapon produced is sufficiently precise to avoid unintended targets and limit collateral damage. We enumerate the control features of the cyber weapon or operation on a *targeting and control*

tableau, listing each control feature by its plane and the targeting attribute to which it pertains. Table II depicts a targeting and control tableau with example entries.

We now analyze the enumerated effects and control features. The goal is to determine if the cyber weapon or operation has sufficient control in terms of Geography, Function and Persona so that its effects are in accordance with the *jus in bello* principles of Discrimination, Distinction, and Proportionality. Considerations of proportionality in a cyber operation should compare with those for kinetic operations. If we would reject some possible collateral damage from a bomb or other kinetic effect, we should reject the same possibility if posed by the cyber operation. Conversely, risks of collateral damage found acceptable for kinetic operations should be similarly acceptable from cyber operations.

If we find the operation complies with the *jus in bello* principles for all its anticipated effects, the operation may lawfully proceed. On the other hand, if we identify noncompliance for one or more effects, it may be possible to modify the control measures to bring the operation into full compliance. Alternatively, it may be necessary to defer operations against a given target until tools and techniques offering sufficient control for their effects are developed or procured. Finally, we may conclude that a given combination of cyber weapon or operation and target do not comply with *jus in bello* principles and that we should consider other alternatives for achieving the military objective.

4. APPLICATION OF THE METHODOLOGY

To further illustrate our methodology, we apply it to W32.Stuxnet, software widely considered to be a cyber weapon. Stuxnet appears to be the best publicly-disclosed example of a potential cyber weapon, with detailed technical analysis readily available [15]. Multiple authors allege that Stuxnet was part of a cyber operation conducted by a state-level actor with the objective of sabotaging Iran's uranium enrichment program. [16-18] Although uncertainty remains about the origin and purpose of Stuxnet, we will assume here that the cyber attack explanation is correct.

We leave to others the question of the lawfulness this operation under *jus ad bellum*. Questions that remain are then: did an attack using Stuxnet constitute lawful armed conflict? Did this cyber weapon include sufficient precision and control of its effects to comply with the *jus in bello* principles of discrimination, distinction and proportionality?

A. Enumeration of Effects

First, we enumerate the likely effects of the operation. Stuxnet exploited multiple vulnerabilities in Windows operating systems to propagate, specifically targeting systems running the Siemens WinCC and SIMATIC Step 7 industrial control system (ICS) software used to manage programmable logic controller (PLC) devices. [15] Stuxnet's primary effect was to alter the operation of certain models of frequency controller, causing them to run the attached device at a very high speed and suddenly bring it to a near stop. This would be likely to damage or destroy devices such as high-speed centrifuges. Altering the intended operation of the frequency

controllers would also have the potential secondary effect of degrading the industrial process controlled. Such manipulation would significantly reduce the yield for a sensitive process such as uranium enrichment. [19]

As secondary effects, Stuxnet replaced or altered components of the WinCC and SIMATIC Step 7 software. Although Stuxnet implanted itself on Windows systems, it had no significant effects on those systems unrelated to gaining access to the target PLCs. Stuxnet also altered frequency converter activity data returned to management systems, ostensibly to mask indications of the primary effects. Table I depicts the effects tableau for Stuxnet.

We infer indirect effects for this operation since these are not coded in Stuxnet. Successful sabotage of the production process could result in a loss of confidence in the reliability of hardware, software and management processes, at least temporarily. A more permanent indirect effect is the possible loss of skilled personnel blamed for production losses or failing to prevent the attack.

TABLE I. EFFECTS TABLEAU FOR STUXNET

	Persistence		
Effect Class	Permanent	Temporary	Transient
Primary	Damage or destroy certain high-speed industrial devices		Alter operation of certain frequency controllers
Secondary	Sabotage industrial process dependent upon precise frequency controller operation	Affect Windows system integrity. Alter components of WinCC and Step 7	Deceive management systems by altering feedback from frequency converters
Indirect	Dismissal or criminal sanctions against management and staff	Loss of confidence in hardware, software or procedures	

B. Enumeration of Target Attributes and Control Features

We must now consider the target attributes and enumerate Stuxnet's control features. As stated above, we accept the hypothesis that the target of Stuxnet was Iranian uranium fuel enrichment facilities. More specifically, the target devices were the industrial control systems and IR-1 centrifuges employed in the uranium enrichment process [20]. What, then, were the attributes of this target?

Geography: the target was known to be located in Iran. Forensic analysis indicated that the initial infections occurred in five Iranian networks, probably from direct connection of portable storage devices [15].

Function: The target devices were industrial control systems carrying out the uranium enrichment process. This required the presence of distinctive controller hardware configurations and specific software to manage and monitor the process. Additionally, the process would

involve behavior, such as high rotational speeds for extended periods of time, differentiating it from more mundane functions.

Persona: the targets were owned and operated by Iranian government entities.

Stuxnet contained multiple features apparently designed to limit its effects to the intended targets. It is likely this was done as much for stealth as to control collateral damage; nonetheless, the controls were included. The most significant control features are related to the target's function and fall within the physical and logical planes. This is understandable since the function of the target in this case is significant and provides more specificity than geography or persona attributes. Stuxnet checks for specific ICS software, hardware and mode of operation before delivering its effects. Stuxnet also includes control features on the supervisory plane that provide some limits on propagation and basic command and control capability [15]. Table II depicts the targeting and control tableau.

TABLE II. TARGETING AND CONTROL TABLEAU FOR STUXNET

	Target Attribute		
Plane	Geography	Function	Persona
Physical	Initial launch via external storage devices connected to five Iranian networks	• Hardware: check for a Siemens PLC, type 6ES7-315-2, using a Profibus communications processor module CP 342-5 • Configuration: The PLC must be connected to at least 33 frequency controllers manufactured by either Fararo Paya (Iran) or Vacon (Finland)	N/A
Logical	N/A	• Software selectivity: Infect only Simatic manager (s7tgtopx.exe) and WinCC project manager (CCProjectMgr.exe) on Win32 • ICS operation: trigger primary effects only if specific operating pattern is observed. (Must operate at 807 Hz to 1210 Hz for 12.8 days, initially)	N/A
Cyber persona	N/A	N/A	N/A
Supervisory	N/A	• Copy limit: after three copies from an external storage device, delete • Temporal: cease propagation if system clock is greater than date in configuration file (June 24, 2012) • Command and Control Server: upon activation on a new host, contact a command and control server (www.mypremierfutbol.com, www.todaysfutbol.com) via HTTP, [provides the opportunity track propagation and to modify or disable the software]	N/A

C. Analysis

After enumerating Stuxnet's effects and control features, we analyze these to determine if it complies with the principles of discrimination, distinction and proportionality.

1. Discrimination and Distinction

Although Stuxnet's propagation methods appear to be rather indiscriminant and lack distinction, its delivery of effects is neither indiscriminant nor lacking in distinction. Stuxnet sought to spread onto a wide range of Windows-based systems, presumably to increase the probability of reaching targets on closed networks. While the supervisory plane control features

provided some limits on the time frame and rate of propagation, Stuxnet was almost certain to propagate onto non-target systems, as was seen in its spread within Iran and beyond [15]. However, Stuxnet appeared to have only temporary, secondary effects on systems without the Siemens ICS software, taking no action beyond attempting to propagate. Conversely, Stuxnet's primary effects were applied with discrimination and distinction. The control features on the physical and logical planes limited delivery of primary effects to the specific combinations of ICS hardware and software suspected to be in use at the target facility and only these devices were functioning in a manner consistent with operating centrifuges for uranium enrichment. This combination of controls enabled Stuxnet to distinguish between targets and kept it from acting as an 'indiscriminant weapon.'

2. Proportionality

The possible collateral damage from Stuxnet's effects was in compliance with the principle of proportionality. Stuxnet was apparently designed to minimize collateral damage. Stuxnet affected only systems running ICS software with only those operating in very specific ways triggering the primary effects. Although there was a possibility of collateral damage to untargeted uranium enrichment facilities, the risk appears to be acceptable for the intended military objective.

As stated previously, we leave for others the question of the legitimacy of resorting to armed force to disrupt Iran's uranium enrichment operations. However, within the context of armed conflict, Stuxnet appears to have incorporated sufficient controls and targeting precision to represent a lawful application of force against this military objective.

5. CONCLUSION

It is apparent that operations in the cyber domain will grow in frequency and potential for collateral damage. Many questions remain regarding the legal issues of operations in the cyber domain and how to conduct these operations in a lawful manner. This paper has introduced a methodology for examining the targeting and control of cyber weapons and operations with respect to lawful armed conflict. This work is a step toward defining a common framework in which policy makers and personnel from the technical and legal disciplines examine these questions. Experience will no doubt enhance our understanding of this problem. It should also lead to better quantification of targets, effects and controls along with more formal processes for evaluation. Finally, the body of international law pertaining to armed conflict may expand to address questions of cyber weapons and operations.

REFERENCES:

[1] M. Schmitt, "Wired warfare: Computer network attack and jus in bello" International Review of the Red Cross, vol. 84, no. 846, June 2002.

[2] M. Sklerov, "Responding to International Cyber Attacks as Acts of War" in Inside Cyber Warfare, J. Carr. O'Reilly, 2009.

[3] T. Wingfield, "International Law and Information Operations" in Cyberpower and National Security, F. Kramer, S. Starr and L. Wentz eds. Potomac Press, 2009.

[4] M. Schmitt, “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework” Columbia Journal of Transnational Law 37: 885, 913–15.
[5] N. Rowe, “The Ethics of Cyber War Attacks.” in Cyber War and Cyber Terrorism, A. Colarik and L. Janczewski, eds. The Idea Group, 2007.
[6] D. Kuehl, “From Cyberspace to Cyberpower” in Cyberpower and National Security, F. Kramer, S. Starr and L. Wentz eds. Potomac Press, 2009.
[7] U.S. Department of Defense, Department of Defense Strategy for Operating in Cyberspace. July, 2011.
[8] R. Clarke and R. Knake, Cyber War: The Next Threat to National Security and What to Do About It. Harper Collins, 2010.
[9] F. Kramer, “Cyberpower and National Security: Policy Recommendations for a Strategic Framework.” in Cyberpower and National Security, F. Kramer, S. Starr and L. Wentz eds. Potomac Press, 2009.
[10] G. Rattray, Strategic Warfare in Cyberspace. MIT Press, 2001.
[11] M. Swanson, et al., Contingency Planning Guide for Federal Information Systems, Special Publication 800-34 Rev. 1. National Institute of Standards and Technology: Gaithersburg, MD, 2010.
[12] U.S. Department of Defense, Joint Publication 3-13: Information Operations. February, 2006.
[13] J. Muir and P. van Oorschot. Internet Geolocation and Evasion, Technical Report TR-06-05, School of Computer Science, Carleton University, April, 2006.
[14] Q. Norton, “Anonymous 101.” Internet: http://www.wired.com/threatlevel/2011/11/anonymous-101. November 8, 2011 [February 1, 2012].
[15] N. Falliere, L. Murchu, and E. Chien, W32.Stuxnet Dossier. Symantec Corp., February, 2011.
[16] G. Brown, “Why Iran Didn’t Admit Stuxnet Was an Attack.” Joint Forces Quarterly, no. 63, October, 2011.
[17] L. Milevski, “Stuxnet and Strategy, A Special Operation in Cyberspace?” Joint Forces Quarterly, no. 63, October, 2011.
[18] S. Weinberger. “Is this the start of Cyberwarfare?” Nature, vol. 474, June, 2011.
[19] D. Albright, P. Brannan, and C. Walrond. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Internet: http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf, December, 2010 [February 1, 2012].
[20] P. Shakarian “Stuxnet: Cyberwar Revolution in Military Affairs.” Small Wars Journal, vol. 7, no. 4, April 2011.