Cyberspace Operations Collateral Damage - Reality or Misconception?

Giorgio Bertoli, CISSP
Dr. Lisa Marvel

ABSTRACT

Practically all military actions have the potential to result in undesirable collateral damage. Laws and international treaties mandate the minimization of civilian casualties and damage to civilian property. To enforce this, the military developed methods and tools to help predict the collateral damage that may result from the employment of specific weapon systems under various conditions. These processes have been refined over time, and are now very effective for the planning of kinetic operations. The emergence of cyberspace as an operational domain, however, adds new complexities. Evaluating the overall impact of a cyberspace weapon is less intuitive and more multifaceted to predict. Cyberspace capabilities have inherent differences in their behavior and employment that require additional study and scrutiny. These complexities, however, have been misconstrued and mythicized to the point where the perceived damage that can result from the utilization of any cyberspace tool is often greatly exaggerated. When decomposed, as part of a holistic collateral damage taxonomy, the processes for quantifying the undesirable effects that may result from the employment of many types of cyberspace weapons is not that much different than from their kinetic counterparts.

Keywords—Collateral Damage, Cyberspace Operations

I. INTRODUCTION

Imagine we have received intelligence confirming that a group of insurgents has established an operations center in the midst of a busy residential area. From within this base of operations, the enemy has created a recruiting campaign leveraging social media. They have also gathered a team of hackers to eavesdrop on local US Army assets and to spread misinformation. The cell is small but effective, and their work is directly impacting the fight. We know we must strike–but how?

Mr. Giorgio Bertoli, CISSP works for the U.S. Army Intelligence and Information Warfare Directorate (I2WD), Communications-Electronics Research Development and Engineering Center (CERDEC), US Army Research Development and Engineering Command (RDECOM), as Senior Scientific Technology Manager (SSTM) of Offensive Cyber Technologies.

With 22 years of federal service, Mr. Bertoli has extensive government experience in Cyber, Electronic Warfare, and military tactics. Mr. Bertoli's research areas include the development of advanced Electronic Warfare (EW), Computer Network Operations (CNO), Cyber, and Quick Reaction Capability (QRC) technologies.

Mr. Bertoli has a Bachelor's and Master's Degree in Electrical Engineering from the New Jersey Institute of Technology, and a second Master's Degree in Computer Science from the University of Massachusetts Amherst. Mr. Bertoli is a Certified Information Systems Security Profession (CISSP). During his 6.5 year Military career, Mr. Bertoli served as a combat Engineer and deployed as part of Operation Desert Shield and Operation Desert Storm.

Within a two-block radius are a dozen houses, six businesses, a hospital, a house of worship and an elementary school. Our Soldiers work to pull together a plan. They know they can use traditional weapons to strike with precision, and they can accurately predict the risk to local civilian populations and property. They discuss the possibility of a cyber offensive, which would reduce risk to the civilian population and minimize the threat to an already precarious environment, but commanders are uncertain of potential unintended outcomes and are limited in their ability to quantify the likelihood of related 2nd and 3rd order effects. Ultimately, they choose the kinetic weapon to engage the target and accept the known risks associated with this course of action.

The ability to accurately predict all potential consequences (both intended and unintended) often govern our decisions on what amount and type of military force to employ. Over the past century, the military has developed effective processes and metrics to quantify the risk associated with the use of kinetic weapons. Now, the advent of cyberspace warfare is providing new challenges where effects are less tangible and more difficult to define in term of "blast radius" and "probability of hit". The resulting uncertainty has over-amplified the perceived risks associated with the employment of cyberspace capabilities.

The execution of any action has associated consequences. Most often, these consequences are intended, and the reason the action was undertaken. Sometimes, however, actions can have other unintended, and often undesirable, effects. Examples of this are easy to find, whether as side effects of certain medications, car accidents as a byproduct of driving, or more relevantly, civilian casualties due to military conflict. We designate all such negative events that can result from a specific action as un-

Dr. Lisa Marvel until her recent retirement, was a researcher with the U.S. Army Research Laboratory (ARL) at Aberdeen Proving Ground, Maryland. Her research interests include coding, communications and cybersecurity. She received her B.S.E.E. degree from the University of Pittsburgh in 1992 and the M.S. and Ph.D. degree in electrical engineering from the University of Delaware in 1996 and 1999, respectively. Lisa holds an Affiliated Faculty position with the Computer and Information Sciences Department at the University of Delaware. Additionally, she was the Agility Lead for the ARL Cyber Security Collaborative Research Alliance (ARL Cyber CRA).

intended consequences. Collateral damage is then a subset of these unintended consequences that can occur as a result of intentionally destructive actions; often used in a military context.

Given most actions can have the potential for unintended results, the mechanism we use to decide if an action is worth taking involves evaluating the associated risk of all potential outcomes. In most cases, for mundane everyday actions, this is a simple process that we perform almost intuitively based on experience. For more complex situations (e.g. project management), a methodology for the evaluation of risk, based on the likelihood that a specific undesirable event will occur, and its associated severity, is commonly used. [1] To ensure accuracy, it is essential that all key factors that can lead to unintended consequences are considered. The root causes of collateral damage can be categorized into a generic higher order taxonomy. This taxonomy can then serve as a useful model for the evaluation of the overall collateral damage risk associated with a specific destructive action.

II. BACKGROUND AND MOTIVATION

In 2011, the Department of Defense identified cyberspace as an operational domain [2]. This designation effectively placed this new, virtual, man-made environment on par with the more tangible physical operational domains of land, air, sea, and space. The need for the US to defend and project power within and through this domain at various echelons have since been codified in emerging doctrine [2][3] and discussed in multiple articles [4][5].

International law and treaties govern military operations in any domain. These laws explicitly state "in the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects" [6]. This legal requirement to minimize collateral damage must also be applied to cyberspace operations. This, however, is not a simple extension from the more familiar physical domains. Cyberspace transcends geographical boundaries. Execution of activities within it are near the speed of light. It is, in many ways, an intangible battlespace in which executed effects are not governed by the laws of physics and, as a result, are hard to predict [7][8]. Given these challenges, it is difficult to measure the risk associated with the execution of an offensive cyberspace capability and to estimate the amount of collateral damage that it may cause. Evidence that our inability to quantify this risk has impeded the employment of cyberspace capabilities has been publicly reported [9], and will undoubtedly continue to limit our capacity to operate within this new domain if not overcome.

There is a prevalent misconception that all cyberspace effects are analogous to biological agents, in that, once released they will propagate and infect others with impunity[1], lending to the belief that they are incapable of precision targeting. This is simply not true in many cases. In addition, there is an inclination for applying a higher standard of fidelity to cyberspace capabilities. Neil Rowe, in his work "The Ethics of Cyberweapons in Warfare," [8] provides one such example.

> Cyber warfare does not target military personnel directly but only their software and data. But usually, cyberattacks will be effective against any computer with the same type of vulnerable software. Military organizations use mostly software that is also used by civilians. So civilian computers could also suffer from military cyberattacks; in fact, they are usually more vulnerable because their countermeasures are not as good.

While this is certainly a true statement, it is hardly unique to cyberspace capabilities. Could you not also claim that a bullet is equally effective against both military and civilian personnel? And, that civilians are actually at greater risk as they lack training, body armor and other protective mechanisms afforded to the military?

The highly technical nature of cyberspace, coupled with overzealous rhetoric by the media and other proponents [10] [11] [12], has resulted in an exaggeration, or often, a downright misrepresentation of the actual risk [13][14][15]. The potential for an offensive cyberspace weapon to cause collateral damage is undeniable; however, while such capabilities are different from their kinetic counterparts, they are not mystical. Many can be well controlled in their function and behavior.

In the rest of this article, we define a general taxonomy for the root causes of collateral damage and compare cyberspace weapons to their more traditional counterparts. We will demonstrate that, in many cases, they are not significantly different, and as such, existing risk assessment approaches can be applied.

[1] The term "computer virus" was coined in 1984 by Frederik Cohen to describe the operation of self-replicating computer programs synonymous to a biological "infection" because of the conceptual similarities in their ability to infect others.

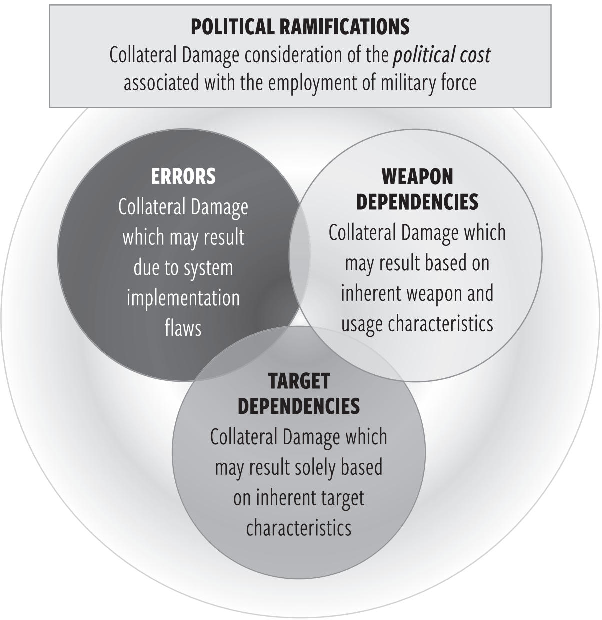
POLITICAL RAMIFICATIONS
Collateral Damage consideration of the *political cost* associated with the employment of military force
ERRORS
Collateral Damage which may result due to system implementation flaws
WEAPON DEPENDENCIES
Collateral Damage which may result based on inherent weapon and usage characteristics
TARGET DEPENDENCIES
Collateral Damage which may result solely based on inherent target characteristics

Figure 1. Generic Collateral Damage Taxonomy

III. GENERIC COLLATERAL DAMAGE TAXONOMY

In general, collateral damage may be categorized into four distinct contributing factors [7][8] (Fig 1).

- *Errors (E):* Reflect the collateral damage that may result due to the presence of design or implementation flaws that leads to unintended system performance.
- *Target Specific Dependencies (TD):* Reflect the collateral damage that may result solely based on properties and dependencies inherent to the target system.
- *Weapon Specific Dependencies (WD):* Represents the collateral damage that may result solely based on the intrinsic properties, execution behavior, or employment methodology of the weapon system.
- *Political Ramifications (P):* Encompass the less tangible political and moral aspects of collateral damage to include considerations of public perception and international backlash, gain/loss equities, as well as ethical national principles.

When combined (Eq. 1), these individual aspects of collateral damage will provide the total collateral damage risk (CDR) associated with a specific action, within the context of the environment in which it is executed.

$$CDR = F(R(E), R(TD), R(WD), R(P)) \qquad (1)$$

Where each sub-risk element R(...) can be computed using the standard "Probability of Occurrence Vs Impact" risk model.

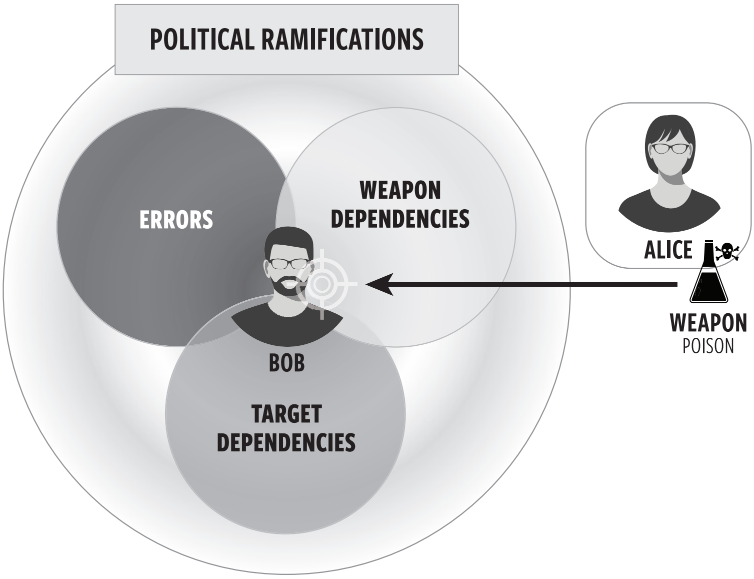

Figure 2. Taxonomy Case Study

IV. SIMPLE ILLUSTRATIVE EXAMPLE

To better illustrate this proposed taxonomy, let us apply it to an intuitive example. In this simple use case (figure 2), Alice (our weapon operator) wishes to poison (the weapon system) Bob (her target).

Given this simple construct, we can consider how each of the four categories within the described risk taxonomy would apply.

- *Errors (E):* The poison could potentially have a flaw. For instance, it may take a much longer time for Bob to die than desired. During this time, others who come in contact with Bob's bodily fluids could also be poisoned themselves. This is clearly collateral damage due to an error or malfunction in the weapon system.
- *Target Specific Dependencies:* What if Bob was a prominent medical researcher? Perhaps Bob was on the cusp of a revolutionary discovery for a new vaccine. As a result of his death, this work can no longer continue and many more people will die from the disease he would have cured. You will note, that this form of collateral damage is completely independent of the weapon system employed. This same outcome would have occurred if Bob had died naturally or by some other means.
- *Weapon Specific Dependencies:* Given this poison must be ingested; Alice decides to contaminate the water supply of the town Bob resides in. As a result, the poison will affect a lot more people beside Bob. This type of collateral damage is only dependent on the weapon system. In this example, specifically in the way it was employed.

- *Political Ramifications:* This last category must take into account other intangible considerations. What will be the international backlash to Bob's death? What if the poison is discovered as a result of an autopsy? Could something in the formulation provide attribution of its creator? Could an antidote now be crafted to prevent Alice from using this poison again? Or worse, could the poison be reverse engineered and then used against others?

V. OFFENSIVE CYBERSPACE CAPABILITY COMPARISON

With a clear understanding of the presented collateral damage taxonomy, we can now address what additional considerations, unique to cyberspace weapons, must be made.

- *Errors:* Historically, programming errors within computer exploits have been a significant source of unintentional disruptive behavior, which in turn directly led to or exacerbated the amount of damage that resulted. It is important to note, however, that exploits "released in the wild" are often developed by relatively unsophisticated programmers who likely have little concern for the collateral damage that may result. This is not the case for professionally developed capabilities. The potential for design or implementation flaws are factors that must be considered by all weapons system. Minimizing this particular source of collateral damage is best done through the implementation of sound development, testing, and validation procedures; guidelines that are already included as part of existing acquisition processes. When such procedures are followed, this risk category should not by any different when applied to cyberspace weapons[2].

- *Target Specific Dependencies:* It may be the case that the execution of a cyberspace effect, which significantly impacts the targeted system, will cause additional unintended damage based on the dependent processes that system controls. A classic example is a hypothetical attack targeting a Programmable Logic Controller (PLC) that manages some step of a greater physical process (e.g., a waste treatment plant, or a manufacturing facility). Altering or limiting the functionality of such a device may disrupt the overall physical process it supports with potentially catastrophic consequences that are both difficult to predict, and that can cascade to cause additional unintended events to occur[3]. Such collateral damage, however, is not a function of the attack mechanisms used[4], but rather is directly related to the target system and the processes it controls[5]. Calculating this aspect of collateral damage must be

[3] As an example, imagine a Cyberattack is conducted against a power generation plant. The exploit shuts down a specific component resulting in a power outage. This (especially if ongoing for extended periods of time) may have significant 2nd and 3rd order ripple effects. Other power plants may also be impacted due to the additional power draw that results as they try to compensate. If streetlights no longer function, traffic conditions can quickly become gridlocked. Local businesses can no longer utilize Point of Sale systems or process credit card payments, which will, in turn, result in financial losses and possibly civil unrest, and so forth.

[4] The same collateral damage would result regardless of the cause for the malfunction (for instance, a mechanical failure or a kinetic strike).

[5] It can be argued, that for this aspect of collateral damage, non-kinetic engagement options have a distinct advantage over more traditional kinetic warfare since any damage caused, to include any potential collateral damage, may be more readily reversed [18].

performed from the perspective of the target system and requires an in depth understanding of all its functions and dependencies.

- *Weapon Specific Dependencies:* Collateral damage can result from the uncontrolled execution of a cyberspace capability. By its inherent design, cyberspace transcends physical boundaries, such as geographical proximity, and can operate on varied time scales (both extremely small and extremely long). As a result, depending on its design, the release of a software application (malicious or otherwise) within this environment may be difficult to restrict its distribution or "spread" can be hard to control or predict. Consequently, a cyberspace effect that is employed against a specific target system may also unintentionally or indiscriminately impact other systems. This is a unique aspect of some cyberspace weapons when compared to their kinetic counterpart.
- *Political Ramifications:* The employment of a cyberspace weapon (with well-defined behavior) will not significantly change this last risk consideration. One exception will be in the determination of equities. Just as in our simple use case, cyberspace effects are often perishable, and their usefulness is significantly decreased once discovered. Also, they may be reverse engineered and repurposed for more nefarious usage by a third party.

In summary, as per table 1, it can be shown that deriving the overall collateral damage risk associated with a cyberspace capability is not markedly different from those of more conventional weapon system.

Collateral Damage Category	Kinetic Weapon System Possible Collateral Damage	Cyber Weapon System Collateral Damage Considerations
ERRORS	Errors can lead to malfunctions that results in civilian casualties property	Errors can lead to malfunctions that results in civilian casualties property
TARGET SPECIFIC DEPENDENCIES	Processes governed by the target system may fail resulting in cascading collateral damage effects.	Processes governed by the target system may fail resulting in cascading collateral damage effects. However, they may be easier to reverse or recover from.
WEAPON SPECIFIC DEPENDENCIES	Weapons have well defined targeting probability and blast radius based on well understood physical and empirical models.	Some cyber weapons may be capable of propagating outside the bounds of the intended target system with harder to predict limitations.
POLITICAL RAMIFICATIONS	Traditional use of force and proportional response considerations	Same plus additional concerns regarding potential loss of weapon effectiveness and possible 3rd party repurposing.

Table 1: Collateral damage consideration comparison between kinetic and cyber weapons

Within this taxonomy, only the "Weapon Specific Dependencies" attribute is significantly unique to cyberspace operations. To identify the risk associated with this specific cause of collateral damage, we must quantify what undesired consequences may occur as a result of the emergent/uncontrolled behavior inherent within a cyberspace weapon's design. While this is sometimes difficult, methods for bounding the amount of damage that can result have been studied [16]. Furthermore, many cyber capabilities significantly limit (or altogether do not possess) the ability to spread beyond the target system, thus negating this risk altogether. It is this facet of "cyber" collateral damage that is overemphasized and often mistakenly intertwined with other risk factors, which are beyond the weapon system's control, that contribute to the misconception that cyberspace capabilities cannot be safely employed in support of military operations [17].

VI. CONCLUSION

As with any military weapon system, consideration for the collateral damage that may occur based on the employment of offensive cyberspace capabilities must be assessed and quantified. Cyberspace effects and tools have unique operational characteristics that present specific challenges for the determination of collateral damage risk. These challenges, however, are not insurmountable. As described, most of the core contributing factors leading to collateral damage are independent of the weapon system used and therefore can leverage already established risk determination processes. Additional work conducted by the Communication-Electronics Research Development and Engineering Center (CERDEC) and Army Research laboratory (ARL) has built upon the taxonomy presented in this paper to develop a methodology for the quantification of the collateral damage potential associated with a specific computer exploit [6][16]. The non-intuitive and highly complex nature of the cyberspace domain has resulted in an overinflated perception of the risk associated with the employment of cyberspace capabilities. In many cases, the use of non-kinetic cyber effects can be well defined and more desirable than their kinetic counterpart.

[6] Please contact the authors of this paper for additional information.

NOTES

1. MITRE, "System Engineering Guide: risk impact assessment and prioritzation," MITRE, [Online]. Available: https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-impact-assessment-and-prioritization, Accessed June 30, 2016.

2. Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," 2011.

3. Depertment of Defense, Joint Publication 3-12(R) - Cyberspace Operations, US Department of Defense, 2013.

4. M. Leed, "Offensive Cyber Capabilities at the Operational Level," Center for Strategic & International Studies, 2013.

5. J. K. Sandborn, "Cyber Steps up its role on the battlefield," *Army Times,* Aug 25, 2014.

6. Department of Defense, Law of War Manual, Washington, DC: OFFICE OF GENERAL COUNSEL, 2015.

7. P. Lin, F. Allhoff and N. Rowe, "Computing Ethics, War 2.0: Cyberweapons and Ethics," *Communications of the ACM,* vol. 55, no. 3, 24-26, 2012.

8. N. C. Rowe, "The Ethics of Cyberweapons in Warfare," *International Journal of Cyberethics,* vol. 1, no. 1, 2009.

9. J. Markoff and T. Shanker, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk," *New York Times,* August 2, 2009.

10. T. Capaccio, "Cyber-Armageddon Less Likely Than Predicted, Clapper Says," 25 2 2015. [Online]. Available: http://www.bloomberg.com/news/articles/2015-02-26/cyber-armageddon-less-likely-than-smaller-attacks-clapper-says.

11. B. Schneier, "The Threat of Cyberwar Has Been Grossly Exaggerated," CNN.com, 7 7 2010. [Online]. Available: http://www.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/.

12. T. Payton, "Cyberwarfare - Fact or Fiction?," 27 8 2010. [Online]. Available: http://www.infosecisland.com/blogview/6845-Cyberwarfare-Fact-or-Fiction.html.

13. T. E. Smith, "Cyber Warfare: A Misrepresentation of the True Cyber Threat," *American Intelligence Journal,* vol. 31, no. 1, 82-85, 2013.

14. S. Lawson, "Beyond Cyber-Doom," Mercatus Center, George Mason University, 2011.

15. K. Fink, J. Jordan and J. Wells, "Considerations for Offensive Cyberspace Operations," *Military Review,* no. May-June, 4-11, 2014.

16. G. Bertoli and L. Marvel, "Collateral Effect Potential Metric for Computer Exploits," Available from giorgio.bertoli.civ@mail.mil, Abberdeen Proving Ground, MD, 2016.

17. C. B. A. Metcalf, "Tactical Cyber: How to Move Forward," *Small Wars Journal,* 2014.

18. N. C. Rowe, "Towards Reversible Cyberattacks," in *Proceedings of the 9th European Confernece on Information Warfare Security,* Thessaloniki, Greece, 2010.