Journal of Strategic Security

Volume 11 | Number 1 Article 4

Defining a Class of Cyber Weapons as WMD: An Examination of the Merits

Benjamin B. Hatch
United States Air Force, benjamin.hatch@yahoo.com

pp. 43-61

Recommended Citation
Hatch, Benjamin B.. "Defining a Class of Cyber Weapons as WMD: An Examination of the Merits." *Journal of Strategic Security* 11, no. 1 (2018): : 43-61.
DOI: https://doi.org/10.5038/1944-0472.11.1.1657
Available at: http://scholarcommons.usf.edu/jss/vol11/iss1/4

Defining a Class of Cyber Weapons as WMD: An Examination of the Merits

Author Biography

Lt Col Benjamin Hatch, USAF, is currently a student at the Air War College, Air University, Maxwell AFB, Alabama. Previous to this assignment, he served at the Pentagon on the Joint Chiefs of Staff in the Deputy Directorate for Global Operations (J-39) where he oversaw specialized support to sensitive plans and joint military operations. A combat veteran of Iraq and Afghanistan, Lt Col Hatch has commanded Air Force Office of Special Investigations (AFOSI) detachments three times. He also completed two staff assignments at Headquarters, Air Force, where he concurrently served as an executive officer for the Air Force Scientific Advisory Board Study on Defense of Forward USAF Bases. He earned a master's degree in Government from Johns Hopkins University in 2008.

Abstract

This article examines the merits of defining a class of offensive destructive cyber weapons as weapons of mass destruction (WMD). It analyzes the growing danger of destructive cyber weapons in the future joint operating environment and the devastating effects they may have in the physical domain. Further, it outlines evidence that specifically coded, offensive destructive cyber weapons would meet the spirit and intent of the three academic conditions for categorization as WMD. It argues the merits of categorizing a class of destructive cyber weapons as WMD, and addresses important factors required to examine advantages afforded to policy makers. Towards this end, the paper offers two recommendations for consideration to account for the value in designating a class of destructive cyber weapons as WMD. The recommendations include a proposed cyber deterrence theory of "Attributed Response Assured," and outline how this theory could support a U.S. cyber policy of strategic ambiguity. Further, it recommends defining acceptable behaviors for cyber activity by the international community. In the absence of a U.N.-led effort, the establishment of a Proliferation Security Initiative-type agreement could further steps to clarify "norms" and communicate "redlines" to potential adversaries. These steps would assist policy makers in the collective effort towards enabling the security of a networked world against the most dangerous cyber threats capable of causing mass casualties or mass destruction.

Disclaimer

JSS

SPRING 2018

JOURNAL OF STRATEGIC SECURITY
VOLUME 11 | ISSUE 1 | ARTICLE 3

DOI: 10.5038/1944-0472.11.1.1657

Defining a Class of Cyber Weapons as WMD: An Examination of the Merits

BENJAMIN B. HATCH
Air War College, Air University, Maxwell AFB, Alabama
benjamin.hatch@yahoo.com

ABSTRACT

This article examines the merits of defining a class of offensive destructive cyber weapons as weapons of mass destruction (WMD). It analyzes the growing danger of destructive cyber weapons in the future joint operating environment and the devastating effects they may have in the physical domain. Further, it outlines evidence that specifically coded, offensive destructive cyber weapons would meet the spirit and intent of the three academic conditions for categorization as WMD. It argues the merits of categorizing a class of destructive cyber weapons as WMD, and addresses important factors required to examine advantages afforded to policy makers. Towards this end, the paper offers two recommendations for consideration to account for the value in designating a class of destructive cyber weapons as WMD. The recommendations include a proposed cyber deterrence theory of "Attributed Response Assured," and outline how this theory could support a U.S. cyber policy of strategic ambiguity. Further, it recommends defining acceptable behaviors for cyber activity by the international community. In the absence of a U.N.-led effort, the establishment of a Proliferation Security Initiative-type agreement could further steps to clarify "norms" and communicate "redlines" to potential adversaries. These steps would assist policy makers in the collective effort towards enabling the security of a networked world against the most dangerous cyber threats capable of causing mass casualties or mass destruction.

Journal of Strategic Security

ISSN: 1944-0464
eISSN: 1944-0472

INTRODUCTION

The destructive potential of unconstrained cyber warfare is a maturing threat that warrants the full attention of defense policy makers. To put the danger and the corresponding policy opportunities in perspective, one can view the emergence of specifically coded offensive destructive cyber weapons in context of the world in 1946. The previous year America had dropped atomic bombs to end World War II, and in the aftermath came the genesis of new strategies and policies on the nature of warfare. Although it proved impossible to foresee the impact atomic weapons would have in constructing new ways of thinking about the future character of war, policy makers fully embraced strategies capable of unleashing the destructive potential of this continuation of politics by yet another means. To avoid the possibility for unconstrained use of offensive cyber weapons capable of causing mass casualties or mass destruction, the United States, in partnership with the international community, should evaluate the emerging role of cyber weapons in the context of the future joint operating environment. Towards that end, this article argues that defining a class of offensive destructive cyber weapons as Weapons of Mass Destruction (WMD) presents multiple advantages to US decision makers, to include advancing international and domestic cyber policy options to defend against and deter cyberattacks purposefully designed to cause mass casualties or mass destruction. This article presents the argument in full acknowledgement that cyber weapons must remain valid tools for future military operations. As such, the argument is limited in scope to those specific offensive destructive cyber weapons designed to cause mass casualties or mass destruction.

A review of the growing danger of destructive cyber weapons is necessary to assess the appropriateness of establishing a class of those weapons as WMD. A key component in addressing this issue is to examine the evolution of offensive destructive cyber weapons and their destructive potential in the physical domain. It is the destructive effects of special weapons that policy makers would normally evaluate for the appropriateness to align them under the WMD umbrella. Finally, it will offer two recommendations to assist policy makers in advancing cyber policy options to defend against and deter cyberattacks purposefully designed to cause mass casualties or destruction. It also proposes a cyber deterrence theory of Attributed Response Assured. Although specific audiences may value the additional details afforded by classified information, the scope of discussion and sources of information in this article are purposefully limited to open source publications in order to enable conversations with a broader audience.

https://doi.org/10.5038/1944-0472.11.1.1657

IS IT A WMD? ASSESSING CYBER'S DESTRUCTIVE POTENTIAL

The question on if the destructive nature of cyber weapons warrants "special" classification as WMD has limited historical context. The Joint Chiefs of Staff (JCS) formally acknowledged the potential for destructive cyber effects in 2004. At the time, the JCS considered associating the destructive potential of cyber weapons to a revised definition of WMD. Limited to a footnote in the 2004 *National Military Strategy* (NMS), the JCS reconceptualized WMD in the broader context of the effects achieved. Towards this end, the Joint Staff introduced the term Weapons of Mass Destruction or Effect (WMD/E). The term WMD/E's expanded definition suggests the NMS authors were attempting to find balance between the known "destructive kinetic effects" of WMD weapons and the "disruptive impact" of more asymmetrical weapons available to terrorists and other aggressive states.[1] At present, the JCS recognizes that offensive actions in and through cyberspace may create degradation, disruption, or destruction effects in the physical domain.[2]

In February 2016, Secretary of Defense Ashton Carter confirmed that the United States was using cyber as a weapon of war. In referencing US military actions against the Islamic State in Syria and Iraq (ISIS), Secretary Carter said, "Just like we drop bombs, we're dropping cyber bombs."[3] While specifics on US cyber capabilities are not available in the open source, the *New York Times* in June 2017 described the United States as using its "most sophisticated offensive cyber operation" where it was targeting ISIS online videos and propaganda.[4] The cyber weapons employed against ISIS denied their computer administrators access to accounts and deleted some content. Cyber weapons described as the "most sophisticated" that change passwords or delete content would seem to support an argument that cyber weapons are intended to be more disruptive than destructive. Open source information suggests, however, that the United States may have cyber weapons with the ability to cause destructive effects in the physical domain, for example malware similar to the Stuxnet malicious code capable of 'blowing up nuclear centrifuges' in Iran, or computer viruses designed to 'sabotage missile launches' in North Korea.[5] The effects of these two attacks would not rise to the level of WMD, but offer context towards the evolving destructive potential of cyber weapons.

The US Intelligence Community appears to support an argument that the intent of cyber weapons are its disruptive effects. Former Director of National Intelligence James Clapper, in testimony to the US Senate in 2016, described cyber as an exploitable domain used by adversaries to conduct "espionage, theft, extortion, and other criminal activities." These activities

ISSN: 1944-0464
eISSN: 1944-0472

do not suggest a destructive effect. Director Clapper acknowledged, however, that Russia and China had "sophisticated cyber programs," and that Iran and North Korea were enhancing their "attack capabilities."[6]

While US security strategies have traditionally highlighted WMD threats from state actors, most notably "rogue states" such as Iran and North Korea, as well as violent extremist organizations who claim to be pursuing nuclear, biological, chemical, or radiological weapons (CBRN), they acknowledge the danger associated with cyber weapons is real and credible. The Trump administration's 2017 *National Security Strategy* acknowledges, "cyberattacks…have the capability to harm large numbers of people and institutions."[7] The 2015 *National Military Strategy* specifically calls out particular concern with the proliferation of "cyber capabilities," referencing this concern in the same sentence as WMD.[8] The 2014 *Quadrennial Defense Review* states the Department of Defense "must be able to defend the Nation from an imminent, destructive cyberattack on vital US interests."[9]

In assessing the destructive potential of cyber weapons, the discussion must avoid focusing on US cyber weapon executions currently restrained by policy or authorities.[10] Lt Gen Jeffrey Harrigian, Commander, US Air Forces Central Command, said in a December 2016 interview that allied countries had the authority to "employ cyber weapons and techniques against ISIS" that US cyber forces were not permitted to execute.[11] As described by the *New York Times*, the restrained use of US cyber weapons against ISIS is purposefully limited in execution by policy to disruptive effects. To assess the threat of employing cyber weapons as WMD more comprehensively, defense policy makers must focus on its destructive capabilities and potential if unconstrained.

There is a single framework available to assess if specific cyber weapons meet the threshold for classification as a WMD. In his book, *Countering WMD*, Air War College Professor and WMD expert Al Mauroni specifies three basic conditions that a for weapon systems should meet to be defined as a WMD.[12] The system's fundamental design is the initial consideration for the system to act as a weapon. To meet this threshold, there are two examples to consider. First, the 2009 Stuxnet worm that damaged the centrifuges involved in Iran's nuclear program is assessed as the "world's first digital weapon" and the code was fundamentally designed to cause physical destruction on equipment controlled by computers.[13] Second, Secretary of Defense Carter's confirmation the United States uses cyber in the form of "cyber bombs" and as a weapon of war further supports an argument cyber code designed to cause destruction in the physical domain has met this initial condition.[14]

The second condition Mauroni set is a determination that the weapon has the "capability to cause mass causalities (defined as more than one thousand injuries or deaths) at a single point in time and space."[15] The DOD Law of Armed Conflict outlines three examples where cyber weapons could be employed to achieve mass casualties. Specifically, cyber operations that:

1. *trigger a nuclear plant meltdown;*
2. *open a dam above a populated area, causing destruction; or*
3. *disable air traffic control services, resulting in airplane crashes.*[16]

These examples demonstrate meeting the second condition.

Mauroni's final condition is that the WMD should be "defined by internationally accepted conventions as a 'special' category of weapons systems."[17] While there is not currently an international convention, there have been attempts to explore such a possibility. The international community has discussed the broader topic, establishing the current international position that international law and in particular, the U.N. Charter is applicable to acts in and through cyberspace, as published in the 2013 U.N. Group of Governmental Experts (UNGGE) consensus report on cyberspace.[18] The UNGGE's subsequent work failed to produce a report that further clarified the legal framework, instead calling for further deliberations.[19] However, the international community's efforts meet the spirit of the third condition for WMD classification.

WHY NOW: EXAMINING THE EVOLUTION OF CYBER WEAPONS

In 2008, the Air Force commissioned a RAND study to review the operational realities of being able to "fly and fight in cyberspace."[20] The resulting product, titled *Cyber Deterrence and Cyberwar*, determined the greatest danger to the United States from cyberspace might be operational rather than strategic. The study's authors concluded, "strategic cyberwar, by itself, would annoy but not disarm an adversary."[21] To engage in strategic cyberwar, RAND argued, is to assume a level of risk that an adversary worthy of such an attack has the capability to respond militarily in ways that would do more than simply annoy. RAND also challenged any assertion that cyber warfare can win a nation's wars independently and decisively. Even if cyber threats were assessed as operational rather than strategic, the report provided a comprehensive argument for why cyber deterrence is necessary to ensure the United States maintains superiority in the information medium. In short, approximately 10 years ago cyber

ISSN: 1944-0464
eISSN: 1944-0472

weapons were perceived as Weapons of Mass Annoyance and the cyber topic in general proved to be a subject defense senior leaders and policy makers struggled to comprehend.

For example, the Air Force Chief of Staff (CSAF) gave a presentation in September 2012 at the Air Force Association's annual conference in Washington DC[22]. During his remarks, the CSAF in part focused on cyber security, an issue he viewed as an Air Force priority. He openly acknowledged and described in colorful details his ignorance on the topic. Air Force Chief of Staff requested cyber professionals "dumb down" briefings and avoid using "cyber talk" so he and other senior leaders could better understand the problem.[23] He predicted it would take 30 years to replace those in the top ranks who lacked a strategic understanding of cyber with experts. It is unlikely this reference disparaged senior leaders, and CSAF's comments were likely purposeful in an attempt to add humor to a discussion made in a public forum. However, the comments suggest that only five years ago there were senior defense leaders who were unprepared to address cyber policy development, or possibly even appreciate the potential role of cyber weapons. Due to the rapid nature of advancements in the cyber domain, it becomes imperative that senior defense leaders have sufficient understanding of how cyber contributes to the defense of America and can articulate the need for new or updates to existing policy.

In June 2014, the National Defense University (NDU) Center for the Study of Weapons of Mass Destruction explored the potential of formally categorizing and recognizing cyber weapons as WMD.[24] Looking forward to the strategic future set in 2030, the authors wrote that it would be inappropriate and possibly disadvantageous to the United States to apply the WMD designation to cyber weapons at the time. Their rationale was the seemingly nascent state of cyber weapon policy and strategy development. Until the United States had a strategy that outlined how to operationalize cyber weapons, it seemed counterintuitive to add the WMD classification to cyber. For in doing so, they assessed there would be risk in prematurely constraining a capability that could in reality maximize flexibility options for decision makers. The NDU article further acknowledged that a cyber WMD treaty would normally be associated with provisions to limit cyber's use, or set in motion steps to eliminate or control certain cyber threats. With all the potential negatives, the report was unable to find any advantages to categorizing cyber as WMD.

Changes in 2015 to the DOD Law of Armed Conflict manual suggest a legal foundation that may support categorizing a class of offensive destructive cyber weapons as WMD. The three examples previously referenced describe scenarios of cyber operations where mass casualties may occur:

http://scholarcommons.usf.edu/jss/vol11/iss1/4
DOI: https://doi.org/10.5038/1944-0472.11.1.1657

Nuclear reactor meltdown, opening a dam near population centers, and causing airplane crashes. A determination would be helpful, as confrontations and crises in and through the cyber domain that have already occurred. In addition to the Stuxnet attack previously described, the media has reported other cyberattacks. Russia conducted a cyberattack and shut down the Ukrainian power grid affecting hundreds of thousands of people. Russia also conducted a denial of service attack against Estonia allegedly for removing a war memorial. North Korea targeted an American entertainment organization due to a movie perceived to portray their supreme leader negatively, leading to significant economic damage. Islamic State in Syria and Iraq has lost much of the claimed territory for its self-proclaimed caliphate; however, it continues to maintain a footprint in the cyber domain. A few months ago, it was reported Russian hackers are targeting US nuclear plants. Consequently, the opportunity has narrowed for further strategic pause to assess the role or debate the merits of defining specific cyber weapons as WMD.

While a destructive cyberattack with WMD-type effects has not yet occurred, the persistently offensive cyber environment suggests it may be the threat of the future.[25] The informed senior leaders of today who acknowledge the value in constraining cyberspace to deter offensive destructive cyberattacks appear to have firm legal footing to add formally, a class of cyber weapons to the WMD category. Armed with an understanding that cyber weapons have evolved beyond Weapons of Mass Annoyance, policy makers can initiate actions immediately by assuming a leadership role to find opportunities for sustainable solutions that may deter the potential use of offensive destructive cyber weapons capable of mass casualties or mass destruction in the future. The following section offers two recommendations for policy makers to consider as they assess the advantages of designating specific cyber weapons as WMD to prepare for these future challenges.

RECOMMENDATION NUMBER 1

Attributed Response Assured: Discussion on Cyber Deterrence

Deterrence is a critical component in mitigating the potential for state and non-state entities to employ cyber weapons capable of WMD-type effects. Furthermore, it can help prevent a dangerous trend of spreading malicious technology, such as destructive cyber weapon coding, from state actors to violent extremist organizations or other "rogue states." It seems probable the United States, in releasing to the media information about the existence of what Secretary Carter called "cyber bombs," purposefully intended for the international community to know that it has offensive

cyber capabilities, as well as the will to employ them. The reason for doing so is likely to enhance its cyber deterrence efforts.

Robert Pape defines deterrence in his book *Bombing to Win* as actions taken to persuade a state from initiating specific actions because the estimated risk of doing so outweighs the perceived benefits.[26] Thomas Schelling's view of deterrence, as described in his book *Arms and Influence*, is the "diplomacy of violence." Put another way, it is the bargaining power behind a credible threat of damage by the stronger party that causes another to yield or comply with demands.[27] In short, a state must communicate its intentions clearly, and its communication must be credible in order for a deterrence strategy to be effective. However, the high-level of sophistication combined with the anonymous nature of the cyber domain adds an additional requirement to the deterrence framework: The state or non-state actor contemplating a cyberattack must be convinced the other party has sufficient digital investigative and forensics capability to attribute the attack to the correct source.

In this light, the challenge is to develop a comprehensive cyber deterrence theory that effectively persuades state and non-state actors from conducting destructive cyberattacks against US interests. To be effective, US cyber deterrence policy must command the attention of the international community so adversaries weigh the ramifications of conducting a destructive cyberattack in their pre-attack calculus. Most importantly, the theory needs to support a desired end state of strategic stability. The cyberattack deterrence policy for state actors may by necessity be different from one focused on violent extremist organizations. Maintaining a principal assertion that non-state actors who resort to cyberwarfare remain engaged in politics by another means it would seem plausible that deterrence could be successful if potential actions were assessed as adversely affecting the organization's ability to achieve its political goals. This line of reasoning is at odds, however, with the presumption that terrorists *cannot* be deterred, a theory endorsed by former President Bush in 2006.[28] Common ground between these two theories is the belief violent extremist organizations conduct attacks, to include cyberattacks, in order to achieve some end. W. Elaine Bunn wrote that defensive deterrence, which correlates to denying non-state actors the benefits of conducting terror-type attack tactics, might be more effective than the Cold War approach of deterrence by punishment.[29] Regardless, both defensive deterrence and deterrence by punishment against non-state actors operating in the cyber domain requires additional examination to maximize any benefits.

The 2015 *DOD Cyber Strategy* clearly states the United States will respond to a cyberattack against its interests. The United States will choose the

time, place, and manner of response, using what is described as the appropriate and lawful instrument of US power.[30] It seems, therefore, the US position on cyberattack response is one of *strategic ambiguity*. The value in ambiguity is that an adversary remains challenged in solving a risk vs. benefit calculus equation. If the adversary wonders what their fate might be, it would likely be deterred from launching a cyberattack. A component of the pre-attack calculus, however, will be an evaluation whether or not the threat of response is credible. According to author Lawrence Freedman, "Credibility was also assumed to be based on how past commitments had been honored."[31]

The US response to the North Korean Sony cyberattack offers some insight into how an adversary may calculate the response credibility of the United States. The *Washington Post* reported President Obama pledged to conduct a "proportional response" to the North Korean cyberattack, and later imposed economic sanctions against their government.[32] The *Post* article further stated the United States decided to take action in a manner it had never done before in "response to a cyberattack by another nation; it named the government responsible and punished it."[33] A public declaration that the White House had not responded until 2015 to a state-sponsored cyberattack does not appear to indicate a precedent of US action taken in response to communicated threats that an adversary would find credible. As most cyberattacks will fall below the threshold of mass destruction, and may not necessarily warrant a military response, the United States should consider clearly establishing a "redline" for response to help bridge any perceived credibility gap.[34]

A metric that specifies the threshold of destructive effects that would warrant a response would be a valuable initial step. While US policy is absent the specific details, the *New York Times* quoted Secretary of Defense Carter as defining a major cyberattack as "something that threatens significant loss of life, destruction of property, or lasting economic damage."[35] The same article continued, citing officials, the United States cares mostly about "the top two percent of all cyberattacks."[36] It is unclear, but probable; Secretary Carter's definition of major cyberattack is not limited to destructive attacks and includes disruptive attacks. As such, some senior defense officials would include cyberattacks used to disrupt a strategic capability, such as missile warning or nuclear command and control, which would blind the United States against incoming missiles or from communicating with our strategic forces, as a major cyberattack.[37] Much like the promise of mutually assured destruction if nuclear weapons were launched, the United States may prevent the destructive effects of a cyberattack by specifying that attacks that cause more than one thousand casualties, the only hard number to define mass casualties in US policy, for

example, would cross America's response threshold.[38] Without clarifying details, there may potentially be undesired actions taken in response to a cyber policy of strategic ambiguity.

An unintended consequence of such a policy is that it may actually invite state and non-state actors to engage in a series of probing cyberattacks in order to test America's will and response preferences. An example is the US cruise missile attacks against al Qaeda camps in the 1990s. Instead of deterring future attacks, they were seen as "another small and cowardly step by a wounded tiger."[39] As a result, if the United States is slow to act or fails to respond proportionately to a cyberattack, it is reasonable to expect state and non-state actors to attempt additional provocative attacks. Communicating clear "red lines" on the use of destructive cyber weapons capable of mass casualties or mass destruction is a necessary step towards an effective deterrence.

The same goes for attribution. If state or non-state actors believe they can conduct cyberattacks anonymously, it may encourage more groups to make cyber capabilities the preferred means to commit destructive acts. There are generally two types of attribution: Technical and geographic source.[40] A robust capability to establish attribution of a WMD-type cyber weapon to a geographic source enables decision makers to hold direct dialogue and focus on response options against a state or non-state actor operating from that area. Technical attribution may be more valuable for attacks emanating from the sovereign territory of a specific nation where the government denies responsibility for an attack attributed to that nation geographically. Therefore, if the United States responds, it would be prudent to conduct a robust information campaign in parallel to the response, highlighting evidence of how the United States confirmed attribution, to maximize any benefits associated with the counterattack. Regardless, effectively deterring cyberattacks will remain the best approach towards enabling the safety and security in the cyber domain. The question for cyber deterrence, therefore, is what theory would best ensure adversaries are deterred from conducting a cyberattack.

The present author has developed a cyber deterrence theory for consideration coined "Attributed Response Assured."[41] This theory seeks to deter WMD-type cyberattacks by reinforcing two conditions: One, it assures adversaries the United States will respond to a cyberattack against its interests that results in mass casualties or mass destruction once attributed to a state or non-state actor, and two, the response will employ all appropriate instruments of national power in any domain. A capability to attribute cyberattacks is the most critical element of this theory as it can persuade an adversary against conducting attacks if their attack calculus included

a perceived ability to hide behind a cloak of anonymity or make it appear another party was responsible. Comparisons in the value of a credible response assurance can be made to the mutually assured destruction theory of nuclear deterrence that specifies neither side would attack if there were a mutual assurance both sides would be destroyed in nuclear war. Attributed Response Assured signals to an adversary that if one dares to launch a WMD-type cyberattack, they can expect the United States to attribute the attack, after which the responsible party will encounter punishing reprisal actions. This approach nests under the 2018 *National Defense Strategy* goal of being strategically predicable, but operationally unpredictable.[42] As necessary, response options for attributed attacks should be considered from the perspective of the adversary to ensure the response maximizes its persuasiveness against future attacks.

The United States may enhance the credibility of its cyber deterrence policy by establishing a class of WMD cyber weapons, and delegating to military commanders at the appropriate level the authority to respond to cyberattacks below the WMD threshold. Delegating authorities would improve integration of cyberspace operations into joint military operations, and thereby enhance the lethality of the joint force. This approach to cyber policy would acknowledge that the most devastating cyberattacks are different in character from most other cyberattacks, and could enable military commanders to respond and react to those attacks that fall outside of the "top two percent" the United States Government cares about the most. Furthermore, delegating the ability to respond to lower-threshold cyberattacks would help reinforce a credible deterrent against WMD-type cyberattacks as the United States would show by word and actions that it has the will to follow through on threats of punishment. Credible punishing response options could include or be limited to law enforcement activity, economic sanctions, or military actions. The response may be overt, clandestine, or covert. A cyber deterrence theory of *Attributed Response Assured* supports a national policy of strategic ambiguity, permitting the broadest spectrum of options for decision makers to respond on a timeline of their choosing.

Another benefit is it helps avoid the potential for strategic miscalculation as it reinforces an understanding that any counterattack would be founded on attributing the source of the attack. It should motivate the international community to share information on cyber threats in order to avoid the potential for wrongful attribution or risk escalation. It also serves to reassure the international community, to include allies and adversaries alike, that the United States will not take action unless or until attribution is confirmed. Conversely, once an attacker's identity is confirmed, potentially involving the use of court-credible digital forensics, an adversary

ISSN: 1944-0464
eISSN: 1944-0472

is assured the United States has the will and capability to respond at a time and place of its choosing, consistent with its national security policy. A sufficient and credible investigative and forensics capability to assess attribution is the foundation of such a deterrence theory. It also places emphasis on developing capacity for a robust cybersecurity posture, further enabling deterrence by denial. Continuing this conversation towards an enduring solution should involve the international community.

RECOMMENDATION NUMBER 2:

International Engagement: Defining Cyber's Role in Strategic Deterrence

As the debate over security in cyberspace continues to resonate, an issue of primary concern should be the recognition that the cyber domain is international space. As such, activity in cyberspace must comply with applicable and relevant elements of international law. For those state or non-state actors who choose to conduct offensive destructive cyberattacks, the effects could then be assessed as falling above or below a specific threshold of acceptable behavior. The United Nations should define that threshold and should initially consider drawing a line at cyber activity that produces WMD-type effects. Once a U.N.-led-international cyber WMD "redline" is established, it becomes clear which actions are unacceptable and warrant a response. However, proposals in the international community to establish even basic "norms" in the cyber domain have stalled, leaving it mostly unregulated. As such, establishing a cyber WMD "norm" within the cyber domain may not be achievable at present through a U.N. led effort.

A US-led approach may be necessary. In prepared remarks, the Trump administration's Homeland Security Advisor Tom Bossart said during the June 2017 "cyber week" conference that following the unsuccessful conclusion to the UNGGE to clarify how international law applies in cyberspace, notably in the areas of self-defense, state responsibility, and countermeasures, that "it's time to consider other approaches."[43] Following recent cyber hacks attributed to Russia it is not shocking to see why Russia, in particular, would not support UNGGE discussions to clarify countermeasures, as it might address how the United States could counterattack within the constraints of international law. Consequently, Bossart proposed working in smaller groups of "likeminded" partners willing to act responsibly in cyberspace and agreeable to hunt out unacceptable behavior and impose costs. He also suggested establishing bilateral agreements.

In the absence of a U.N.-led initiative, the following framework for cyber is recommended to build upon previous successful 'coalition of the willing' agreements to address WMD proliferation. In 2003, the Bush White House

established a Proliferation Security Initiative (PSI) that sought a "coalition of nations" to use existing international and domestic laws to disrupt the transport of nuclear, biological, or chemical weapons and associated technologies to state and non-state actors suspected of building a WMD program.[44] There was no international treaty; rather the PSI relied upon collaboration between member parties. Participating states then intercepted ships at sea or at domestic ports so the cargo could be inspected for WMD components. In 2005, National Security Advisor Condoleezza Rice briefed that in two years' time the 60 countries supporting the PSI had successfully stopped some WMD trafficking, including a minimum of 11 interdictions that helped prevent Iran and others from procuring material to enable its missile and nuclear programs, which contributed to the "unraveling of the A.Q. Kahn network."[45]

The PSI framework could be an effective means to move the cyberattack discussion forward internationally. Actions taken by participating nations would set a precedent of accepted behavior within the international community. It may further present decision space for key states, to include the United States, Russia, and China, to discuss differences in opinions over "norms" in cyberspace openly. At best, it affords more opportunities through tangible and observable acts to establish cyber "norms" with those countries viewed as potential US adversaries.

SUMMARY AND CONCLUSIONS

This article analyzed the growing danger of destructive cyber weapons in the future joint operating environment and the devastating effects they may have in the physical domain. Further, it outlined evidence that specifically coded, offensive destructive cyber weapons would meet the spirit and intent of the three academic conditions for categorization as WMD. It argued the merits of categorizing a class of destructive cyber weapons as WMD, and addressed important factors required to examine advantages afforded to policy makers. Towards this end, the article offered two recommendations for consideration to account for the value in designating a class of destructive cyber weapons as WMD. The recommendations included a proposed cyber deterrence theory of "Attributed Response Assured," and outlined how this theory could support a US cyber policy of strategic ambiguity. Further, it recommended defining acceptable behaviors for cyber activity by the international community. In the absence of a U.N.-led effort, the establishment of a Proliferation Security Initiative-type agreement could further progress to clarify "norms" and communicates, "redlines." This progress would assist policy makers in the collective effort towards enabling the security of a networked world against the most dangerous cyber threats.

ISSN: 1944-0464
eISSN: 1944-0472

A more secure cyberspace deters against the potential for future attacks capable of mass casualties or mass destruction. States and non-state actors considering a cyberattack, but who find network security measures too difficult to bypass, may pursue alternate behaviors. This approach is the foundation of a policy of deterrence by denial. Yet, sophisticated adversaries may still be able to find ways to exploit vulnerabilities. The key to deterrence is communicating to those considering WMD-class cyberattacks that the United States has the capability to establish attribution and the political will to respond at a time and place of their choosing. Equally important is building the credibility of those threats. Policy makers should consider delegating to US military commanders limited authority to respond to cyberattacks below the WMD threshold as a means towards enhanced credibility. The adversary must be effectively persuaded that the cost of conducting a cyberattack is too severe. These are critical elements of the proposed cyber deterrence theory of attributed response assured.

A sustainable deterrence requires international support. While the international community has not yet formally established a convention categorizing cyber as a "special" weapon, it has taken steps to define "norms" for activity in a free and open internet. The international community, with the United States in a leadership role, must take action to establish common understanding on what constitutes the differences between criminal activity and the top two percent of cyberattacks that concern the DOD. While the international debate continues, the United States government, as one option, could establish national policy to define a specific class of offensive destructive cyber weapons as WMD. This designation could lead the international community towards a decision point on a cyber convention. Formal recognition by the international community on cyber "norms" will clearly communicate the accepted thresholds of cyber warfare, can build a foundation of deterrence, and help reduce the risk of unconstrained escalation.

Other benefits that require further examination outside the limits of this article is if the WMD categorization would better enable senior leaders to establish policies to manage the consequences of a successful attack resulting in mass casualties. Consistent with other WMD policies, it would likely also set in motion a requirement for the DOD and other government stakeholders to organize, train, exercise, equip, and prepare adequate response plans to destructive cyberattacks.[46] Resources could then be allocated and focused to account for and address the spectrum of response options for these threats. The September 2017 Dragon-17 exercise in Warsaw, Poland, included a test of NATO and Polish cybersecurity practices, and may be worth evaluating for areas to potentially benchmark in other military exercises.[47]

The cyber WMD designation also requires further examination to assess if it may positively influence military equipment acquisition and procurement processes. It could drive a requirement to establish within applicable DOD policy publications, which may include the Manual for the Operation of the Joint Capabilities Integration and Development System, a category for US weapon systems to be designated as "cyber mission critical" similar to the current "CBRN mission critical" designation.[48] Such a designation would enhance the resiliency and survivability of systems and crews to withstand the effects of a destructive cyberattack without losing the ability to accomplish the assigned mission. A "cyber mission critical" designation would act as a forcing function for the services to account for cyber resiliency and avoid acquisition of systems with cyber vulnerabilities. The importance of cyber resiliency was highlighted in August 2017, as the US Army had to issue an order to stop using specific drone aircraft procured from a Chinese manufacturer, as they were vulnerable to cyber malware.[49]

While the greater issue of cyber is vast and complex, limiting it at present to the destructive potential of specific cyber weapons affords the opportunity to focus on the most dangerous malicious code, while avoiding likely contentious discussions related to broader cyber topics. These actions align with the DOD strategic goal of "being prepared to defend the US homeland and US vital interests from disruptive or destructive cyberattacks of significant consequence" as outlined in the *2015 DOD Cyber Strategy*.[50] Policy makers can find multiple advantages that enable efforts to meet this goal by designating a class of specific offensive destructive cyber weapons as WMD. Similar to the collective efforts since 1946 to deter the use of nuclear weapons, history will likely judge the decision favorably if an outcome includes effectively deterring the use of unconstrained cyber weapons resulting in mass casualties or mass destruction.

ABOUT THE AUTHOR

Lt Col Benjamin Hatch, USAF, is currently a student at the Air War College, Air University, Maxwell AFB, Alabama. Previous to this assignment, he served at the Pentagon on the Joint Chiefs of Staff in the Deputy Directorate for Global Operations (J-39) where he oversaw specialized support to sensitive plans and joint military operations. A combat veteran of Iraq and Afghanistan, Lt Col Hatch has commanded Air Force Office of Special Investigations (AFOSI) detachments three times. He also completed two staff assignments at Headquarters, Air Force, where he concurrently

ISSN: 1944-0464
eISSN: 1944-0472

served as an executive officer for the Air Force Scientific Advisory Board Study on Defense of Forward USAF Bases. He earned a master's degree in Government from Johns Hopkins University in 2008.

ENDNOTES

1 W. Seth Carus, "*Defining Weapons of Mass Destruction*," (Washington, DC: National Defense University, 2012), 33, available at: http://wmdcenter.ndu.edu/Publications/Publication-View/Article/626547/defining-weapons-of-mass-destruction-revised/.

2 Joint Publication 3-12, *Cyberspace Operations*, February 5, 2013, available at: https://www.hsdl.org/?abstract&did=758858.

3 Ash Carter, "In Fight Against ISIS, U.S. Adds Cyber Tools," interview by Rachel Martin, NPR, February 28, 2016, audio, available at: http://www.npr.org/templates/transcript/transcript.php?storyId=468446138.

4 David E. Sanger and Eric Schmitt, "U.S. Cyberweapons, Used Against Iran and North Korea, Are a Disappointment Against ISIS," *The New York Times*, June 12, 2017. https://www.nytimes.com/2017/06/12/world/middleeast/isis-cyber.html.

5 Sanger and Schmitt.

6 Director of National Intelligence, "Worldwide Threat Assessment of the US Intelligence Community," February 9, 2016, available at: https://www.dni.gov/files/documents/2016-02-09SASC_open_threat_hearing_transcript.pdf.

7 2017 National Security Strategy, 31, available at: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

8 2015 National Military Strategy, 3, available at: https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf; The Department of Defense released the unclassified summary of the 2018 National Defense Strategy in January 2018. As details in the 2018 strategy are classified, this article references the unclassified summary available at: https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

9 Department of Defense, *Quadrennial Defense Review*, (Washington D.C.: Government Printing Office, 2014), 14-15.

10 The Department of Defense *Cyber Strategy*, April 2015, states the United States will always conduct cyber operations under a doctrine of restraint, as required to protect human lives and to prevent the destruction of property, 6.

11 Sanger and Eric Schmitt, "U.S. Cyberweapons."

12 Al Mauroni, *Countering Weapons of Mass Destruction: Assessing the U.S. Government's Policy* (New York: Rowman & Littlefield, 2016), 36.

13 Kim Zetter, "An Unprecedented Look at Stuxnet, The World's First Digital Weapon," *Wired*, November 3, 2014, available at: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

14 Ash Carter, "In Fight."

15 Mauroni, 36, 42; There are conflicting definitions of mass casualty events in policy. The Department of Health and Human Services is the only official United States Government source that specifies a number of casualties to qualify as a mass casualty event, the 1000 casualty threshold as referenced in Mauroni's book on page 42. For a generic definition, see also World Health Organization: A mass casualty incident as "an event which generates more patients at one time than locally available resources can manage using routine procedures. It requires exceptional emergency arrangements and additional or extraordinary assistance. It can also be defined as any event resulting in a number of victims large enough to disrupt the normal course of emergency and health care services (PAHO/WHO 2001)," 6, available at: www.who.int/hac/techguidance/MCM_guidelines_inside_final.pdf; In addition, policy makers should consider Mauroni's proposed flexible definition of "mass casualties" to guide future discussions on WMD and cyber WMD policy and strategy development. He suggests a general scale with three types of mass casualty events: Type A - Between 100 and 1000 casualties (for example the Aum Shinrikyo Tokyo subway incident); Type B – Between 1000 and 5000 casualties (for example the 9/11 incident); Type C – Between 5000 and 50000 casualties (for example a low-yield nuclear weapon), 43.

16 Department of Defense Law of War Manual, *Cyber Operations and Jus ad Bellum*, (Washington D.C: Government Printing Office, June 2015, Updated December 2016), 998, available at: https://www.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190.

17 Mauroni, 36.

18 Tim Maurer and Jason Healey, "What It'll Take to Forge Peace in Cyberspace," *Christian Science Monitor*, (March 20, 2017), available at: http://carnegieendowment.org/2017/03/20/what-it-ll-take-to-forge-peace-in-cyberspace-pub-68351.

19 Michele G. Marfkoff, Deputy Coordinator for Cyber Issues, U.S. Department of State, New York City, "Explanation of Position at the Conclusion of the 2016-2017 U.N. Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, June 23, 2017, available at: https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm.

20 Martin C. Libicki, *Cyber Deterrence and Cyberwar*, RAND Report FA7014-06-C-001 (Santa Monica, CA: RAND, 2009), available at: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

21 Libicki, "Cyber Deterrence."

22 Michael Hoffman, "Cyber Security, an Air Force Punchline?" *Defensetech*, September 26, 2012, available at: https://www.defensetech.org/2012/09/26/cyber-security-an-air-force-punchline/.

23 Hoffman, "Cyber Security."

24 John Caves and Seth Carus, *The Future of Weapons of Mass Destruction: Their Nature and Role in 2030* (Fort McNair, DC: NDU, 2014), 7, available at: http://ndupress.ndu.edu/Portals/68/Documents/occasional/cswmd/CSWMD_OccationalPaper-10.pdf.

25 Dr. Richard Harknett's article states "actors have engaged in increasingly aggressive cyber operations" and he argues a position that deterrence has a better chance of succeeding if more counterattacks are conducted. In doing so, it "will better position the U.S. to shape cyberspace toward both more secure contexts and less aggressive behaviors," available at: https://www.fifthdomain.com/home/2017/07/19/meet-the-scholar-challenging-the-cyber-deterrence-paradigm/.

26 Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca: Cornell University Press, 1996), 12.

27 Thomas Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966), 1-3.

28 George W. Bush, "Commencement Address at the United States Military Academy at West Point," May 27, 2006, available at: http://www.presidency.ucsb.edu/ws/?pid=83.

29 W. Elaine Bunn, "Force, Preemption, and WMD Proliferation." In *Combating Weapons of Mass Destruction*, edited by Nathan E. Busch and Daniel H. Joyner, 156 - 174. Athens: University of Georgia Press, 2009).

30 2015 Department of Defense, *Cyber Strategy*, 11.

31 Lawrence Freedman, *Deterrence*, 3rd edition, (Malden: Polity Press, 2008), 36.

32 Ellen Nakashima, "Why the Sony Hack Drew an Unprecedented U.S. Response Against North Korea," *Washington Post,* January 15, 2015, available at: https://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html?utm_term=.df45abad4c9d.

33 Nakashima, "Why the Sony Hack."

34 The National Defense Authorization Act for Fiscal Year 2018 specifies the policy of the United States on Cyberspace, Cybersecurity, and Cyber warfare is to deter and respond when necessary to "any and all cyberattacks or other malicious cyber activities that target United States interests with the intent to cause casualties among United States persons or persons of our allies; significantly disrupt the normal functioning of United States democratic society or government (including attacks against critical infrastructure that could damage systems used to provide key services to the public or government; threaten the command and control of the United States Armed Forces, the freedom of maneuver of the United States Armed Force, or the industrial base or other infrastructure on which the United States Armed Forces rely to defend United States interests and commitments; or achieve an effect, whether individually or in aggregate, comparable to an armed attack or imperil a vital interest of the United States," see Section 1633, pages 1017-1018, available at: https://www.congress.gov/115/crpt/hrpt404/CRPT-115hrpt404.pdf

35 David Sanger, "Pentagon Announces New Strategy for Cyberwarfare," *New York Times,* April 23, 2015, available at: https://www.nytimes.com/2015/04/24/us/politics/pentagon-announces-new-cyberwarfare-strategy.html.

36 Sanger, "Pentagon Announces."

37 Senior Pentagon Official, Email correspondence to author in September 2017.

38 Mauroni, 42.

39 Jonathan Schachter, "Understanding al-Qa'idah: Power, Perception, and the Powell Doctrine," unpublished research paper, RAND, 2002, as cited in Brad Roberts, "Deterrence and WMD Terrorism: Calibrating its Potential Contributions to Risk Reduction," Institute for Defense Analyses, 2007, 14, available at: http://www.dtic.mil/get-tr-doc/pdf?AD=ADA470305.

40 Jason Healey in *Beyond Attribution: Seeking National Responsibility for Cyber Attacks* discusses the differences between technical attribution and finding the responsible party. He proposes ten categories in the spectrum of state responsibility to help analysts assign responsibility for a particular cyberattack, or campaign of attacks, with more precision and transparency, available at: http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF.

41 Al Mauroni states in his book *Countering Weapons of Mass Destruction* that "cyber deterrence theory has yet to be developed," 174. See also the National Defense Authorization Act for Fiscal Year 2018, "The House bill contained a provision (sec. 1658) that requires the Secretary of Defense to develop a definition of 'deterrence' to be used in the context of cyber operations," and the Senate amendment also contained a provision "(sec. 1630A) that required...a report on various approaches to cyber deterrence," 1046, available at: https://www.congress.gov/115/crpt/hrpt404/CRPT-115hrpt404.pdf.

42 2018 *National Defense Strategy*, 5, available at: https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

43 Thomas P. Bossert, "Remarks by Homeland Security Advisor Thomas P. Bossert at Cyber Week 2017" (speech, Tel Aviv, Israel, June 26, 2017), available at: https://www.whitehouse.gov/the-press-office/2017/06/26/remarks-homeland-security-advisor-thomas-p-bossert-cyber-week-2017.

44 Mauroni, 128-129.

45 Condoleezza Rice, "Remarks on the Second Anniversary of the Proliferation Security Initiative" (speech, Washington D.C., May 31, 2005), available at: https://2001-2009.state.gov/secretary/rm/2005/46951.htm.

46 Department of Defense Directive 2060.02, *Combating Weapons of Mass Destruction (WMD) Policy*, January 27, 2017, outlines service counter WMD requirements, available at: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/206002_dodd_2017.pdf.

47 Associated Press, "Poland, NATO Troops Hold Drills Amid Security Concerns," AP News, September 21, 2017, available at: https://www.apnews.com/4fe2cceef2a442ca96e5eec5c599aef1/Poland,-NATO-troops-hold-drills-amid-security-concerns.

48 Joint Capabilities Integration and Development System (JCIDS) Manual, page D-C-3, Appendix C to Enclosure D, available at: http://www.acqnotes.com/wp-content/uploads/2014/09/Manual-for-the-Operationsof-the-Joint-Capabilities-Integration-and-Development-System-JCIDS-18-Dec-2015.pdf.

49 Melanie Burton, "Australia Okays Use of China Drones in Non-Classified Operations," *Reuters*, September 22, 2017, available at: https://www.reuters.com/article/us-australia-drone/australia-okays-use-of-china-drones-in-non-classifed-operations-idUSKCN1BX0MY.

50 2015 *Cyber Strategy,* 8.