Journal of Strategic Security

Volume 8
Number 4 *Volume 8, No. 4: Winter 2015*

Article 2

# Deterring and Dissuading Cyberterrorism

John J. Klein
*ANSER*, johnjordanklein@aol.com



pp. 23-38

**Recommended Citation**
Klein, John J.. "Deterring and Dissuading Cyberterrorism." *Journal of Strategic Security* 8, no. 4 (2015) : 23-38.
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1460
Available at: https://scholarcommons.usf.edu/jss/vol8/iss4/2

# Introduction

Since the beginning of his Administration, President Barack Obama has stated that cybersecurity is one of the most important challenges facing the United States.[1] In doing so, he noted the irony that the very technologies used by the United States that enable great achievements can also be used to undermine its security and inflict harm on its citizens. For instance, the same information technologies and defense systems that make the U.S. military so advanced are themselves targeted by hackers from China and Russia, potentially leading to increased vulnerabilities. Consequently, ongoing and persistent cyberattacks are considered a threat to U.S. national security.[2]

Included in this overall cybersecurity challenge that President Obama addressed is the threat posed by cyberterrorism. Unfortunately, while being written about since the early 2000's, cyberterrorism is a concept whose definition is still not fully agreed upon. Confusion over cyberterrorism stems, in part, from recent attempts to stretch the concept to include hacktivism and terrorists' use of the Internet to facilitate conventional terrorist actions.[3] Furthermore, some strategists and policy makers believe that acts of cyberterrorism, by either states or non-state actors, may prove to be undeterrable.[4]

This view, however, is incorrect or, at best, a half-truth.[5] Based upon the lessons of history and how conflict in the other media of warfare has unfolded, the credible threat of overwhelming force or other severe actions can, under the right conditions, deter potential attackers from initiating a path of direct confrontation.

## Cyberspace and Cyberterrorism

---

[1] Office of the Press Secretary, *Fact Sheet: Administration Cybersecurity Efforts 2015* (Washington, D.C.: The White House, July 9, 2015) available at: *https://www.whitehouse.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015*.

[2] President Barack Obama, "Remarks by the President at the Cybersecurity and Consumer Protection Summit," Stanford University, February 13, 2015, available at: *https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit*.

[3] Michael Kenney, "Cyber-Terrorism in a Post-Stuxnet World," *Orbis* 59:1 (2015): 111-128, available at: *http://www.sciencedirect.com/science/article/pii/S0030438714000787*.

[4] Lewis, Jim, "Speech on the Role of Deterrence," *Space Security Symposium*, Stimson Center, November 15, 2012, available at: *http://www.stimson.org/about/news/jim-lewis-of-csis-speaks-at-stimson-on-cyber-deterrence/*.

[5] Gray, Colin S., *National Security Dilemmas: Challenges & Opportunities* (Dulles, VA: Potomac Books, Inc., 2009), 62.

The cyber domain, or cyberspace, has been defined by Andrew Krepinevich as:

> "[the world's] computer networks, both open and closed, to include the computers themselves, the transactional networks that send data regarding financial transactions, and the networks comprising control systems that enable machines to interact with one another."[6]

As such, the cyber domain utilizes expansive lines of communication involving a global network, along with hubs of activity at server farms or network hardware locations.[7] Cyber activities involve international commerce and finance, social media, information sharing, and more recently, military-led activities.[8]

When considering whether or how acts of terrorism in the cyber domain can be deterred, the definition of cyberterrorism provided by Dorothy Denning in 2000 before the House Armed Services Committee proves useful.

> "Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not."[9]

---

[6] Andrew F.Krepinevich, "Cyber Warfare: A 'Nuclear Option'?" *Center for Strategic and Budgetary Assessments*, 2012, p. 8, available at: *http://csbaonline.org/publications/2012/08/cyber-warfare-a-nuclear-option/*.
[7] John J. Klein, "Some Principles of Cyber Strategy," *International Relations and Security Network*, August 21, 2014, available at: *http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=182955*.
[8] David E. Sanger, David Barboza, and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *NYTimes.com*, available at: *http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all&_r=0*.
[9] Dorothy Denning, "Cyberterrorism," Testimony to the Special Oversight Panel on Terrorism, Committee on Armed Services, *U.S. House of Representatives*, *U.S. House of*



https://scholarcommons.usf.edu/jss/vol8/iss4/2
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1460

Under this "severity of effects" determination, computer attacks that are limited in scope, but that lead to death, injury, extended power outages, airplane crashes, water contamination, or major loss of confidence in portions of the economy may also qualify as cyberterrorism.[10]

When considering the definition above, cyberterrorism does not include acts of hacktivism. *Hacktivism* is a term used by many scholars to describe the marriage of hacking with political activism.[11] Similar to the actions of hackers, hacktivism includes activities conducted online and covertly that seek to reveal, manipulate, or otherwise exploit vulnerabilities in computer operating systems and other software. Differing from hacktivists, those considered solely as hackers do not necessarily have political agendas.[12]

Hacktivism, though motivated for political reasons, does not amount to cyberterrorism. While hacktivists typically seek to disrupt Internet traffic or computer networks as a form of public protest, they do not typically want to kill, maim, or terrify in the process.[13] The recent successes of hacktivists, however, do highlight the potential threat of cyberterrorism in that a few individuals with little to no moral restraint may use methods similar to hackers to wreak havoc, generate fear, and cause severe injury or death.[14] The line between cyberterrorism and hacktivism, however, may sometimes blur. This is could be especially true if terrorist groups are able to recruit or hire computer-savvy hacktivists for their cause or if hacktivists decide to escalate their actions by attacking the systems that operate critical elements of the national infrastructure, such as electric power networks and emergency services.[15]

Security experts have argued for some time that the energy sector has become a potential target for cyberattack through the creation of Internet links—both physical and wireless—that interfere with the supervisory control and data acquisition (SCADA) systems used by electrical and power distribution

---

*Representatives*, May 23, 2000, available at: *www.stealth-iss.com/documents/pdf/cyberterrorism.pdf*.

[10] Dorothy Denning, "Is Cyber Terror Next?" *Social Science Research Council*, November 2001, available at: *http://essays.ssrc.org/sept11/essays/denning.htm*.

[11] Wiemann, Gabriel, *Cyberterrorism: How Real Is the Threat?* (Washington, D.C.: United States Institute of Peace, December 2004): 4, available at: *http://www.usip.org/sites/default/files/sr119.pdf*.

[12] Ibid.

[13] Ibid., 5.

[14] Ibid.

[15] Ibid.

networks.[16] SCADA systems manage the flow of electricity and natural gas, while also being used to control the industrial systems and facilities used by chemical processing plants, water purification and water delivery operations, wastewater management facilities, and a host of manufacturing firms.[17] Studies have indicated that critical infrastructures that include SCADA systems may be vulnerable to a cyberterrorist attack because the infrastructure and the computer systems used are highly complex, making it effectively impossible to eliminate all potential weaknesses.[18] It is believed by many security professionals that a terrorist's ability to control, disrupt, or alter the command and monitoring functions performed by SCADA systems could threaten regional or national security.[19]

Cyberterrorism, when considered generally, may be conducted by either state or non-state actors, but the calculus and implications can be quite different for each category. Of note, the U.S. Department of State lists three designated state sponsors of terrorism in 2015: Iran, Sudan, and Syria.[20] State sponsored cyberterrorism would most likely be conducted to achieve the goals as defined by the state's political leadership and any actions would tend to support long-term national security goals. Even though the cyber domain offers a bit of anonymity, if a cyberattack is traced back to its network source or Internet address, then the physical location of those perpetrating the attack could be determined within the boundaries of the state authorizing the cyberattack. Because states have geographic boundaries and the initiating computer networks potentially have a physical location, there is increased likelihood, when compared to non-state actors, that those responsible for initiating a state-sponsored cyberattack would be identified.

In contrast, non-state actors—to include many terrorist organizations—do not necessarily act uniformly or according to the same underlying beliefs, and

---

[16] Wilson, Clay, *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*, CRS Report RJ32114 (Washington, D.C.: Library of Congress, Congressional Research Service, October 17, 2003): 12-13, available at: *http://webcache.googleusercontent.com/search?q=cache:2JlpsJ6zCi8J:fas.org/irp/crs/RL32114.pdf+&cd=5&hl=en&ct=clnk&gl=us*.

[17] Stouffer, Keith, Joe Falco, Karen Kent, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security* (Washington, D.C.: U.S. Department of Commerce, 2006): 2-1, available at: *http://www.dhs.gov/sites/default/files/publications/csd-nist-guidetosupervisoryanddataccquisition-scadaandindustrialcontrolsystemssecurity-2007.pdf*.

[18] Weimann, "Cyberterrorism," 6.

[19] Ibid., 7.

[20] U.S. Department of State, "State Sponsors of Terrorism," *State.gov*, available at: *http://www.state.gov/j/ct/list/c14151.htm*.



https://scholarcommons.usf.edu/jss/vol8/iss4/2
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1460

many of the most aggressive organizations are motivated by an ideology that embraces martyrdom and an apocalyptic vision.[21] This ideology may be based on religion or a desire to overthrow a government. Terrorists who are motivated by ideology and intend to conduct cyberattacks against the United States or its interests may not care about the repercussions following an act of cyberterrorism, whether military in scope or not. In such a scenario, some strategists think a terrorist organization's leadership may prove undeterrable by traditional military means.[22] Despite the disparate motivators of terrorists, many terrorist organizations, to include al-Qaida and the self-proclaimed Islamic State, are said by some security experts to function strategically and rationally.[23] Because a terrorist organization's leadership may be inclined to make rational decisions, deterrence may at times be a suitable method of influencing future actions. Consequently, deterrence should be considered a critical element in a successful national strategy to prevent cyberterrorism.

## The Advantages of Cyberterrorism

There are several advantages to using the cyber domain to conduct acts of terrorism. First, cyberterrorism can be far less expensive than traditional terrorist methods.[24] Potentially, all that is needed is a personal computer and an Internet connection, instead of needing to buy weapons, like guns or explosives, or acquire transportation.[25] Second, cyberterrorism has the potential for being more anonymous than traditional, kinetic methods.[26] It can be difficult for security and police agencies to track down the identity of terrorists when they use online "screen names" or are an unidentified "guest user."[27] Third, the number of potential targets is enormous when compared to the number of targets typically used in kinetic actions. The cyberterrorist could target the computer networks of governments, individuals, public utilities, private airlines, SCADA systems, and other critical networks. The sheer number of potential cyber targets is thought to increase the likelihood

[21] Payne, Keith B., *How Much is Enough?: A Goal-Driven Approach to Defining Key Principles* (Fairfax, VA: National Institute for Public Policy, 2009), 5.
[22] Executive Office of the President, *The National Security Strategy of the United States* (Washington, D.C.: White House, May 2002), 15, available at: *http://www.state.gov/documents/organization/63562.pdf*.
[23] Gray, *National Security Dilemmas*, 72.
[24] Weimann, "Cyberterrorism," 6.
[25] In contrast, some experts argue that sophisticated cyberattacks would require greater expense and expertise. See Thomas M. Chen, *Cyberterrorism after Stutxnet* (Carlisle Barracks, PA: United States Army War College Press, June 2014), 22-23, available at: *http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1211.pdf*.
[26] Ibid., 10.
[27] Weimann, "Cyberterrorism," 6.

that an adversary can find a weakness or vulnerability in one of the different networks to exploit. Finally, cyberterrorism can be conducted remotely, a feature that may be especially appealing to some would-be attackers.

## An Exaggerated Threat?

Many critics have noted, however, that while the potential threat of cyberterrorism is alarming and despite all the dire predictions of impending attack, no single instance of real cyberterrorism has been recorded.[28] To date, there has been no recorded instance of cyberterrorism on U.S. public facilities, transportation systems, nuclear power plants, power grids, or other key components of the national infrastructure. While cyberattacks on critical components of the national infrastructure are not uncommon, such attacks have not been conducted in a manner to cause the kind of damage or severity of effects that would qualify as cyberterrorism.[29] The 2007 widespread denial of service cyberattack in Estonia, which brought down the banking system for three weeks, did not cause catastrophic damage, injury, or death.[30] Even in the case of the Stuxnet malware, discovered in June 2010 and called "world's first digital weapon" because of its capability of causing physical destruction to computers and other equipment, did not cause widespread, severe destructive effects.[31]

This begs the question: Just how real is the cyberterrorism threat? While cyberterrorism may be an attractive option for modern terrorists who value its remote access, anonymity, potential to inflict massive damage, and psychological impact, some critics say that cyber fears have been exaggerated.[32] Furthermore, there is disagreement among some cyber experts about whether critical infrastructure computers, to include SCADA systems, offer an effective target for furthering terrorists' goals.[33]

Many computer security experts do not believe that it is possible to use the Internet to inflict damage, injury, or death on a large scale.[34] Some of these experts note that critical computer systems are resilient to attack through the

[28] Chen, *Cyberterrorism after Stutxnet*, 20.
[29] Ibid.
[30] Jason Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," *International Affairs Review*, available at: *http://www.iar-gwu.org/node/65*.
[31] Dan Holden, "Is Cyber-Terrorism the New Normal," *Wired*, available at: *http://www.wired.com/insights/2015/01/is-cyber-terrorism-the-new-normal/*.
[32] Weimann, "Cyberterrorism," 8.
[33] Clay, *Computer Attack and Cyber Terrorism*, 12.
[34] Weimann, "Cyberterrorism," 8.



https://scholarcommons.usf.edu/jss/vol8/iss4/2
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1460

investments of time, money, and expertise during the design and development of these critical systems. For example, the U.S. Department of Defense, Central Intelligence Agency, and Federal Bureau of Investigation are reported to protect their most critical systems by isolating—also called air-gapping—them from the Internet and other internal computer networks.[35]

Despite the ongoing debate about whether the cyberterrorism threat is exaggerated or if the potential destructive effects can be sufficiently achieved to warrant concern, both the news media and government reporting indicate that some terrorist organizations now use the Internet to communicate, recruit people, raise funds, and coordinate future attacks.[36] Even though there is no publically available information that terrorist organizations have directly and successfully attacked Internet servers or major computer networks, reporting does suggest that many terrorist organizations would employ cyber means to achieve their goals if the opportunity presented itself.[37] Because there appears to be a persistent desire by some terrorist organizations to use any and all means, including cyberattacks, to achieve their desired goals, it is paramount for policy makers and military planners to take preparatory actions to prevent such acts and mitigate any effects should such an attack occur. These preparatory actions include deterrence efforts.

## Deterrence and the Law of Armed Conflict

In a frequently cited definition, deterrence is "persuading a potential enemy that it is in his own interest to avoid certain courses of action."[38] The underlying basis of cyber deterrence theory—a subset of general deterrence—is that credible and potentially overwhelming force or other actions against any would-be adversary is sufficient to deter most potential aggressors from conducting cyberattacks, including those acts considered to be cyberterrorism. When considering deterrence in the cyber domain, it is worth considering the advice of Colin Gray, "Given that deterrence can only work, when it does, in the minds of enemy leaders, it is their worldview, not ours, that must determine whether or not deterrence succeeds."[39] Therefore, to deter a potential adversary, we must deter its leadership or decision makers.

---

[35] Joshua Green, "The Myth of Cyberterrorism," *Washington Monthly* (November 2002), available at: *http://www.washingtonmonthly.com/features/2001/0211.green.html*.
[36] Kenney, *Cyber-Terrorism in a Post-Stuxtnet World*.
[37] Chen, *Cyberterrorism after Stutxnet*, 13.
[38] Schelling, Thomas, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960), 9.
[39] Gray, *National Security Dilemmas*, 56.

According to deterrence theory, deterrence only works if there is a credible threat of retaliatory action or force. What is considered a credible retaliatory action within the U.S. defense community is typically governed by the Law of Armed Conflict (LOAC), which is sometimes also referred to as the Law of War. While not directive or preventive of any future action, the ideas and principles within the LOAC have relevance when considering any response to terrorism, including those in response to cyberterrorism.

The LOAC has been defined as the part of international law that regulates the conduct of armed hostilities.[40] The LOAC is based on two main sources. The first is customary international law arising out of hostilities and binding on all states, and the second is international treaty law arising from international treaties, which binds only those states that ratified a particular treaty.[41] The purpose of the LOAC is to reduce the damage and casualties of any conflict; protect combatants and noncombatants from unnecessary suffering; safeguard the fundamental rights of combatants and noncombatants; and make it easier to restore peace after the conflict's conclusion.

Two principles contained in the Law of Armed Conflict are most germane to a follow-on act of cyberterrorism, and these are the principles of military necessity and lawful targeting. The first principle, military necessity, calls for using only that degree and kind of force required for the partial or complete submission of the enemy, while considering the minimum expenditure of time, life, and physical resources.[42] This principle is designed to limit the application of force required for carrying out lawful military purposes. Although the principle of military necessity recognizes that some collateral damage and incidental injury to civilians may occur when a legitimate military target is attacked, it does not excuse the destruction of lives and property disproportionate to the military advantage to be gained.[43]

The second principle, lawful targeting, is based on three assumptions: a belligerent's right to injure the enemy is not unlimited; targeting civilian populations for attack is prohibited; and combatants must be distinguished

[40] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1–02 (Washington, DC: November 8, 2010), 214, available at: *http://ra.defense.gov/Portals/56/Documents/rtm/jp1_02.pdf*.
[41] U.S. Department of the Navy, *The Commander's Handbook on the Law of Naval Operations*, NWP 1–14M (Washington, DC: July 2007), 6–5, available at: *http://www.lawofwar.org/naval_warfare_publication_N-114M.htm*.
[42] Ibid.
[43] Ibid. This concept is also referred to as the principle of proportionality.



https://scholarcommons.usf.edu/jss/vol8/iss4/2
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1460

from noncombatants to spare noncombatants injury as much as possible.[44] Consequently, under the principle of lawful targeting, all "reasonable precautions" must be taken to ensure that only military objectives are targeted in order to avoid, as much as possible, damage to civilian objects (collateral damage) and death and injury to civilians (incidental injury).[45]

An offshoot of the concept of deterrence is extended deterrence, which is currently a topic of study and discussion within the U.S. Department of Defense. "Extended deterrence" refers to strengthening regional deterrence and reassuring U.S. allies and partners through the credible threat of retaliatory force.[46] U.S. Strategic Command, which oversees U.S. Cyber Command, recently held a conference to discuss and assess the Defense Department's ability to deter specific state and non-state actors from conducting cyberattacks of significant consequence on the U.S. homeland and against U.S. interests, to include attacks resulting in loss of life, significant destruction of property, or significant impact on U.S. economic and foreign interests.[47] A topic of the conference also included identifying ways to deter Russia, China, Iran and North Korea from conducting cyberattacks against international allies, which is the realm of extended deterrence.[48] Based upon hundreds of years of treaty precedence, extended deterrence seems to be a viable strategic concept in cyberspace. Article 51, for example, of the Charter of the United Nations acknowledges collective self-defense as an inherent right of one or more states.[49] States being part of an extended deterrence agreement, or collective self-defense treaty, should serve as a means of discouraging conflict or as a means of coming to the defense of allies should deterrence fail. This concept is still relevant in cyberspace.

## Suitable Responses to Cyberterrorism

Based upon the principles of military necessity and lawful targeting mentioned previously, a military response to cyberterrorism should only target and attack military objectives. Military objectives are combatants and those objects which, by their nature, location, purpose, or use, effectively

---

[44] Ibid., 8-1.
[45] Ibid.
[46] This definition is taken from the context of nuclear extended deterrence. See The Department of Defense, *Nuclear Posture Review Report* (Washington, D.C.: April 2010).
[47] "U.S. Military Symposium Will Mull Role of 'Extended Deterrence' In Cyberspace," *Inside Defense*, July 27, 2015.
[48] Ibid.
[49] Article 51, *Charter of the United Nations and Statute of the International Court of Justice* (San Francisco, CA: United Nations, 1945), available at: *https://treaties.un.org/doc/publication/ctc/uncharter.pdf*.

contribute to the enemy's war-fighting or war-sustaining capability.[50] They also include objects whose total or partial destruction, capture, or neutralization would constitute a definite military advantage to the attacker under the circumstances at the time of the attack.[51] Additionally, when considering the cyber-related military objects to target and attack, it is important to understand that it is not unlawful to cause incidental injury to civilians, or collateral damage to civilian objects, during an attack upon a legitimate military objective. Incidental injury or collateral damage must not, however, be excessive in light of the military advantage anticipated by the attack.[52]

Related to the principles within the LOAC, in February 2003, the Bush administration published a report titled "The National Strategy to Secure Cyberspace" that stated the U.S. government reserves the right to respond "in an appropriate manner" if the United States comes under computer attack.[53] This response could involve the use of U.S. cyber weapons or malicious code designed to attack and disrupt the targeted computer systems of an adversary.[54] For any follow-on U.S. military actions to be considered "appropriate," these actions would need to be conducted in the spirit of the LOAC.

So, the question to be answered is what specifically is or is not an appropriate response following an act of cyberterrorism? First, taking into account degree and kind of force required for the partial or complete submission of the enemy, any response—whether kinetic or cyber—should not be considered excessive or disproportionate to the military advantage to be gained. Consequently, if the aggressor's cyberattack caused injury or death to a dozen people, and a resulting cyber counter-attack caused injury or death to a thousand people, with little correlation to a military advantage or gain, then it appears such a situation would not be appropriate within the context of the LOAC. Second, taking into account that a counter-attack to cyberterrorism should target the military objectives contributing to the enemy's war-fighting or war-sustaining capability, then disabling or damaging the adversary's network servers and computer infrastructure, which are routinely used by the

[50] U.S. Department of the Navy, *The Commander's Handbook on the Law of Naval Operations*, para 8.1.1.
[51] Ibid.
[52] Ibid., para. 8.1.2.1.
[53] Executive Office of the President, *The Strategy to Secure* Cyberspace (Washington, D.C.: White House, 2003), 50, available at: *https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf*.
[54] Clay, *Computer Attack and Cyber Terrorism*, 18-19.



https://scholarcommons.usf.edu/jss/vol8/iss4/2
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1460

aggressor to conduct attacks, would seem to be in agreement with the tenets of the LOAC.

A response to a cyberattack does not need to be military in nature, but may entail nonmilitary actions, such as economic or financial measures. For example, in light of the inordinate and ever growing number of cyberattacks against U.S. systems reaching a threshold to consider a national emergency, President Obama issued an executive order in April 2015, seeking to negatively affect the finances of those behind the attacks. The President's executive order states:

> "Starting today, we're giving notice to those who pose significant threats to our security or economy by damaging our critical infrastructure, disrupting or hijacking our computer networks, or stealing the trade secrets of American companies or the personal information of American citizens for profit."[55]

The executive order gives the U.S. Department of Treasury the authority to impose sanctions on individuals or entities responsible for cyberattacks and cyber espionage. In effect, the order allows the freezing of assets when passing through the U.S. financial system and prohibiting those responsible for the cyberattacks from transacting with U.S. companies.

## Counterarguments

There are several counterarguments to the contention that deterrence is effective against cyberterrorism. Jim Lewis, for example, has argued that deterrence will not work in the cyber domain.[56] Lewis states that asymmetric vulnerability to attack, new classes of opponents with very different tolerance of risk, and the difficulty of crafting a proportional and credible response all erode the ability to deter in the cyber and space domains.[57] He notes that public and private entities in the United States experience cyberattacks on a

[55] Michael Daniel, "Our Latest Tool to Combat Cyber Attacks: What You Need to Know," *The White House Blog*, April 1, 2015: available at: *https://www.whitehouse.gov/blog/2015/04/01/our-latest-tool-combat-cyber-attacks-what-you-need-know*.
[56] Stimson Center, "Jim Lewis of CSIS Speaks at Stimson on Cyber Deterrence," *Stimson.org*, November 15, 2012, available at: *http://www.stimson.org/about/news/jim-lewis-of-csis-speaks-at-stimson-on-cyber-deterrence/*.
[57] Ibid.

daily basis, and if these attacks are deterrable, then the U.S. government is doing a terrible job of leveraging our capabilities.[58]

Other critics argue that the use of cyber weapons in response to an act of cyber aggression could cause effects that are widespread and severe, thereby exceeding the guidance of the LOAC.[59] These resulting effects of cyber weapons may be difficult to limit or control. There is the fear that if a computer software attack is targeted against a terrorist group, then it is possible that the malicious code might inadvertently spread throughout the Internet. This could severely affect or shut down critical infrastructure systems in other non-combatant countries, including perhaps computers operated by the United States and its allies and partners.

Still other critics say that choosing an actual target for a military response following an act of cyberterrorism instigated by a non-state actor could prove problematic, since non-state sponsored terrorists may not have clear geographic boundaries, making it difficult to avoid affecting civilians. The critical civilian computer systems within the country hosting the terrorist group may be adversely affected by a U.S. cyberattack against the terrorists' computers and network, thereby resulting in effects that are noncompliant with the principle of lawful targeting. This exact problem is why some strategists and policymakers have long argued that deterrence is ineffective against terrorist leadership, since it could appear that a credible response following a cyberterrorism may not be viable.

Finally, other critics could point out that the United States and other countries would not be bound by the LOAC following a cyberattack by terrorists because terrorists are unlawful combatants who do not follow the LOAC's provisions. After all, unlawful combatants are by definition individuals who directly participate in hostilities without being authorized by a governmental authority, and non-state-sponsored terrorists fall in this category. Nevertheless, any U.S. response to a cyberattack by terrorists—that is, by unlawful combatants—should follow the LOAC's tenets. Indeed, the LOAC addresses terrorist actions specifically by noting that unlawful combatants who engage in hostilities are in violation of the LOAC and in

[58] Ibid.
[59] Clay, *Computer Attack and Cyber Terrorism*, 19.



https://scholarcommons.usf.edu/jss/vol8/iss4/2
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1460

doing so become lawful targets.[60] Consequently, such terrorists may be killed or wounded and, if captured, may be tried as war criminals for their actions.[61]

## A Holistic Strategy of Prevention

The goal of a strategy seeking to prevent an act of cyberterrorism is to cause the leadership of an organization to decide that an attack is not worth the cost or that the attack will fail in achieving the desired objectives. As a result, this strategy of prevention should lead these leaders or decision makers to not choose an act of cyberterrorism. While a credible threat of a military response or force is necessary for deterrence to be effective, any means available to achieve this goal of prevention should be considered part of a suitable strategy. Specifically, other means could include nonmilitary activities if they support discouraging a potential adversary from pursuing an act of cyberterrorism. Consequently, an overall strategy of prevention should include both military and nonmilitary approaches that integrate and layer activities. Such a strategy represents a holistic approach for dealing with the threat of cyberterrorism. These military and nonmilitary activities working together to support the goal of prevention can be categorized as *deterrence* and *dissuasion*.

### *Deterrence*

As previously addressed and despite its limitations in affecting the decision-making calculus of a few leaders, deterrence remains a viable concept for discouraging cyberterrorism. Many terrorist organizations, including al-Qaida and the Islamic State, are thought to function strategically and rationally.[62] For this reason, deterrence is still a relevant consideration. There is nothing within the LOAC that explicitly prohibits a military response to an act of cyberterrorism, even one that is non-state sponsored. As long as the principles of military necessity and lawful targeting are duly considered, both military and nonmilitary responses are viable options.

By conducting persistent and aggressive counterterrorism operations to seek out the most militant terrorist organizations, the United States can increase a potential adversary's perception that there would be a credible threat of force and unacceptable consequence following any attack against the United States.

---

[60] International Committee of the Red Cross, "The Relevance of IHL in the Context of Terrorism," (Geneva, Switzerland: ICRC, January 1, 2011), available at: *https://www.icrc.org/eng/resources/documents/misc/terrorism-ihl-210705.htm*.
[61] U.S. Department of the Navy, *The Commander's Handbook on the Law of Naval Operations*, para. 12.7.1.
[62] Gray, *National Security Dilemmas*, 72.

If Islamic State or al-Qaida's leadership believed that following an act of cyberterrorism the United States would systematically seek them through military or nonmilitary mean and threaten their survival and power base, they might be deterred from conducting a life threatening cyberattack.

In the case of state-sponsored cyberterrorism, the knowledge that the United States has the option to respond "in an appropriate manner" to a cyberattack may increase the likelihood of deterring states that are involved in cyberterrorism. Therefore, if a hostile state enables terrorists to conduct cyberattacks against the United States or its interests, a U.S. response may include both cyber and non-cyber options. While the problems inherent in selecting a suitable military objective associated with an act of non-state-sponsored terrorism have been noted previously, these problems are mitigated in a scenario involving a supporting or facilitating state, because clear geographic boundaries facilitate taking reasonable precautions to help ensure that collateral damage and incidental injury are avoided as much as possible.

*Dissuasion*

Besides deterrence, the other part of a holistic strategy is dissuasion, which seeks to influence the leadership of potential adversaries by discouraging the initiation of military competition.[63] To be effective, dissuasion activities must occur before a threat manifests itself. Dissuasion includes "shaping activities," which are typically nonmilitary in scope and conducted during peacetime.[64] Within the lexicon of the U.S. military services, dissuasion is said to work outside the potential threat of military action. A strategy incorporating dissuasion to influence potential cyber adversaries would seek to convey the futility of cyberattacks, thereby causing a potential adversary's leadership not to seek a military confrontation.[65] Worth noting is that some strategists think that those dissuaded from competing with the United States should not need to be deterred.[66] With respect to dissuading those considering cyberattacks, such an approach should focus on three areas: resilience, forensics, and monetary interception.

[63] Department of Defense, *Annual Report to the President and the Congress* (Washington, D.C.: 2002), 18.
[64] Chairman, Joint Chiefs of Staff, *Combating Weapons of Mass Destruction*, JP 3–40 (Washington, D.C.: Department of Defense, June 10, 2009), x.
[65] Chairman, Joint Chiefs of Staff, *Combating Weapons of Mass Destruction*, I–3.
[66] Gray, *National Security Dilemmas*, 59.



https://scholarcommons.usf.edu/jss/vol8/iss4/2
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1460

Resilience efforts, such as those encompassing redundant network hardware and Internet connectivity pathways, hold promise in making a notable improvement in situations following a widespread and potentially devastating cyberattack. Significant preparations that improve cyber resilience and mitigate and manage the consequences following an act of cyberterrorism can cause an adversary's leadership to determine that a cyberattack will not cause the desired destructive effects. Consequently, if an adversary's leadership determines that a cyberattack is unlikely to achieve their objectives, they may refrain from conducting such an attack in the first place, or decide to pursue another path of causing destruction, such as conventional kinetic attacks.

The second aspect of dissuasion is having a reliable and responsive cyber forensics capability. As defined here, cyber forensics is the science of analyzing and determining the origination source and pathway of a cyberattack after such an attack has occurred, for law enforcement or defense counterintelligence purposes. After an act of cyberterrorism, post-attack cyber forensics capabilities will attempt to use any "electronic fingerprints" or other network and software information to facilitate an attribution determination regarding the source and identity of those responsible for launching the cyberattack. Admittedly, identification and follow-on attribution can be difficult tasks because attackers can use computer intermediaries or channel their attack through anonymizing proxies that hide their Internet protocol address.[67] Nonetheless, a robust and publically-known capability to identify and attribute the source of cyberattack could dissuade prospective cyberterrorists or those supporting their efforts. A successful identification and attribution of a cyberattack may lead to prosecution through civilian courts, or for more significant acts of aggression, lead to targeting with kinetic or non-kinetic weapons.

The last area for dissuading cyberterrorism involves aggressive efforts to intercept and minimize the funding streams used by those involved in cyberterrorism. Such intercepting actions may also be called counter threat finance and sanction activities.[68] Funding is acknowledged as being critical to sustaining the activities of many organization involved in terrorism, to include non-state actors. In the past, such funding to terrorist organizations has come through charities, illegal activities, and front companies. Persistent multinational fiscal interdiction efforts could significantly reduce the funding available to organizations that are most likely to conduct cyberterrorism.

---

[67] Chen, *Cyberterrorism after Stutxnet*, 4.
[68] U.S. Department of State "Counter Threat Finance and Sanctions," *State.gov*, available at: *http://www.state.gov/e/eb/tfs/*.

Current U.S. Department of State counter threat finance and sanction activities seek to target those financial transactions benefiting terrorist organizations, whether coming from states, nongovernmental organizations, or private entities.[69] A sustained effort to eliminate or minimize funding sources used by terrorist organizations could help curtail future recruits for the organization's cause. When combined with cyber resilience and forensics efforts, a terrorist organization's leaders may decide not to seek a direct confrontation through cyberterrorism.

## Conclusion

When dissuasion works with deterrence as part of a broad strategy of prevention, there is an increased likelihood of discouraging a potential adversary's leadership from pursuing acts of cyberterrorism. History suggests, however, that deterrence will at times fail due to miscalculation, uncertainty, or chance. This may also be the case for deterring acts of cyberterrorisms. If deterrence fails and an attack occurs, having measures in place to manage the consequences of a widespread and destructive cyberattack could reduce or limit the damage. A side benefit of a strategy incorporating both deterrence and dissuasion concepts is that a broader range of potential state adversaries may be deterred or dissuaded from conducting relatively "routine" or commonplace cyberattacks on the United States or its interests, because it would seem doubtful that the desired effects can be achieved or that such an attack was worth the cost. Perhaps paradoxically, it has been observed that the success in "the 'war on terror' is likely to make terrorists turn increasingly to unconventional weapons such as cyberterrorism."[70] While some terrorism experts have concluded that, at least for now, truck bombs, terrorist financing, and recruitment seem to pose a greater threat than cyberterrorism, the potential cyberterrorism threat cannot be ignored.

Even though an act of cyberterrorism may seem improbable, many considered the 9/11 attacks improbable beforehand as well. Countless ordinary citizens and politicians within the United States regret that more was not done to improve counterterrorism capabilities and strategies before the 9/11 attacks, especially since many of the needed improvements seemed obvious afterwards. Likewise, the time is now to act in implementing a sound and comprehensive strategy to deter and dissuade cyberterrorism, and not after such an attack has occurred.

---

[69] Ibid.
[70] Weimann, "Cyberterrorism," 11.



https://scholarcommons.usf.edu/jss/vol8/iss4/2
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1460