Air Force Institute of Technology

CSCE 525: Introduction to Cyber Warfare and Security

Nathan Flack

12 October 2018

CTC 6

**Question: Provide a critique for “Limiting…”**

The authors of this article discuss the technical and policy considerations needed to develop and employ targeted cyber weapons. Targeted means that they can be employed with accuracy and without unintended consequences. The paper, “seeks to examine the technical requirements necessary to ensure cyber weapons are not indiscriminate, and the policy guidelines to ensure that outcome.”[[1]](#footnote-1) The authors offer a definition of a cyber weapon as “a software-based IT artifact or tool that can cause a destructive, damaging, or degrading effects on the system or network against which it is directed.”[[2]](#footnote-2) This definition is helpful, although many other variations of a definition exist without a clear consensus in the cyber community. One difference that I would question is the use of cyber weapon to describe the act of data exfiltration while conducting cyber exploitation. I believe this type of cyber action would fall more appropriately under cyber espionage, which should be kept separate from cyber weapons and cyberattack.

They continue their discussion by boiling down the two requirements for a targeted cyberattack. Specifically, cyber weapons can be used discriminately if they can be directed at specific targets and minimize negative effects on non-targeted entities. These two requirements make a lot of sense and are needed if we are going to argue for the use of cyber weapons in light of the Law of Armed Conflict and Geneva Conventions. Another important point is that intelligence of a target must be built into cyber weapons. Meaning the time between target identification and strike must be significantly more than with conventional weapons. I agree with this statement in cases where the weapon must be autonomous. However, if attack is conducted manually cyber operators will have the opportunity to adapt to challenges and variables that were unknown during the planning phase of an operation.

The authors tease out the truth that policy objectives surrounding the prevention of proliferation of cyber weapons may take precedence over using a specific weapon in a certain context. Stuxnet is a clear example of how a specific cyber weapon can be modified or augmented and then reused by the original victim of the attack or other actors in cyberspace for their purposes. This reflects the reality that in cyber, once a capability or weapon is released (or maybe the best word is “spent”) then it may lose future effectiveness or be used in ways the attacker did not intend. However, this article describes several techniques that cyber actors may take to limit or avoid proliferation. This article is a step in the right direction to help governments develop strategies based on the capabilities of cyber weapons. Nations and their governments must work out both the advantages and limitations of cyber weapons and how they are willing to use them across the spectrum of conflict. As James Acton writes, “it may take decades…for states to understand the limitations of cyber weapons and whether and how these limitations can be overcome.”[[3]](#footnote-3)

1. Steven M. Bellovin, Susan Landau, and Herbert S. Lin, "Limiting the undesired impact of cyber weapons: technical requirements and policy implications," *Journal of Cybersecurity* 3, no. 1 (2017): 60. [↑](#footnote-ref-1)
2. Ibid. [↑](#footnote-ref-2)
3. George Perkovich and Ariel E. Levite, eds. *Understanding Cyber Conflict: Fourteen Analogies*, Georgetown University Press, 2017, 57. [↑](#footnote-ref-3)