information security matters

State-on-state Cyberconflicts

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

In the second quarter of 2016, a colleague shared with me an article and a database titled "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–11," written by Brandon Valeriano of the University of Glasgow and Ryan C. Maness of the University of Illinois.[1] It was published in the *Journal of Peace Research* in April 2014. Now, I suspect that the readership of that fine journal and the one you are reading now do not overlap to a great extent, so I will summarize their work and then give my opinions on the subjects they raise.[2]

Importantly, Valeriano and Maness are writing about a specific subset of all cyberattacks, those initiated by a state on the resources of another state, including their private sector organizations and individuals as well as governmental resources. This study examines only actions taken by a government as the initiator of a cyberincident.[3] It addresses the period from 2001 through 2011, stopping at that point to ensure extensive analysis of all incidents and disputes.[4]

Steven J. Ross, CISA, CISSP, MBCP
Is executive principal of Risk Masters International LLC. Ross has been writing one of the *Journal*'s most popular columns since 1998. He can be reached at stross@riskmastersintl.com.

Along with their article, the authors published their information set so that any reader can re-create and, perhaps, extend their analysis.[5] Surprisingly, at least to me, they found only 111 cyberincidents in the period of their research, which they distinguish from cyberdisputes, of which there were 45. They make the differentiation that "Cyber incidents are individual operations launched against a state. Cyber disputes are specific campaigns between two states using cyber tactics during a particular time period and can contain one to several incidents, often including an initial engagement and responses."[6] According to their figures, the most frequent initiator was China; the most frequent target was Pakistan.[7]

Valeriano and Maness are to be congratulated for the thoroughness of their research and the thoughtfulness of their analysis. However, I disagree with their conclusions or, as they put them, their "hypotheses."

But what is the purpose of critiquing an article already three years old in a journal that few ISACA® members have ever heard of, much less read? My rationale begins with the recent statement issued by the G7 Summit in May 2016, which equates state-on-state cyberactivities with acts of war.[8] The people who plan for and respond to government-initiated cyberincidents may very well read the *Journal of Peace Research,* and they are treading into an area where ISACA constituents have significant knowledge and awareness of the current state of both risk and preparedness. So we, too, have a right to be heard on this important topic.

Granted, I have the advantage of knowing about five additional years of cyberincidents, as reported in the media. And perhaps 2011 represented a marked upturn in state-on-state activity. But inasmuch as their hypotheses are stated in future terms, I feel comfortable in extrapolating my own conclusions from the available data.

Hypothesis 1

Due to restraint dynamics, the observed rate and number of cyberoperations between rivals is likely to be minimal. It seems to me that recent events have shown no slowing in the incidence of cyberdisputes. What we lack is definitiveness as to whether the

actions taken were instigated by governments or by individuals acting with state acquiescence, if not outright support. Was it the North Korean government that stole and destroyed information from Sony?[9] Did Russian officials steal emails from the US Democratic National Committee during an election year?[10] Were the distributed denial-of-service (DDoS) incidents suffered by the Philippines after the ruling against China's territorial claims in the South China Sea carried out by the state or by self-styled, but unsanctioned, "patriots"?[11] We will probably never know.

With that proviso, I do not believe that there has been, nor will there be, any diminution in the rate of cyberoperations, whatever those might be. The United States has a Cyber Command in its military, China has a centralized command reporting to the Central Military Commission,[12] the European Union's European Network and Information Security Agency (ENISA) is combatting cyberattacks,[13] and Russia has so-called Information Troops.[14] Anyone who believes that these organizations are for defensive purposes only is, in my opinion, quite naïve.

A more legitimate question is whether any state would carry out a cyber-first strike. I believe that a state would, in the proper circumstances, in which it felt that its vital national interests or even existence are threatened. That is, cyber "weapons" might be used in situations where it was felt that a target state was preparing to use physical, rather than information, force. The Stuxnet attacks on Iranian nuclear facilities, addressed in the Valeriano-Maness study, fit that mold.

Hypothesis 2

When cyberoperations and incidents do occur, they will be of minimal impact and severity due to restraint dynamics. Much of this assertion depends on the definition of "minimal." If the comparison is with the damage caused by World War II, then true enough, cyberincidents thus far have been minimal. But if, for instance, a US presidential election were to be disrupted by cyberattacks, I would consider that a rather severe impact which, in turn, could lead to more serious military consequences.

Valeriano and Maness dismiss this possibility by saying that "offensive states will choose tactics that are easily hidden and free of direct responsibility."[15] The fact that states will seek plausible deniability does not minimize the chance that they will initiate such incidents. Nor does it reduce the possibility that the targeted state will conclude that a state-sponsored incident had occurred and retaliate, setting off an escalation of incidents of greater and greater severity.

"Cyber 'weapons' might be used in situations where it was felt that a target state was preparing to use physical, rather than information, force."

Hypothesis 3

Cyberincidents and disputes that do occur will likely be limited to regional interactions. This hypothesis is the most difficult for me to understand or agree with. In their own analysis covering the period from 2001 through 2011, they report incidents between the United States and Iran, which are certainly not regional. Moreover, governments are generally likely to engage in disputes with neighboring countries, which makes the hypothesis self-fulfilling.

In addition, the Internet has made the entire world one great region, with virtually every action against a given state having repercussions in interactions with other states. These days, no island is an island, entire of itself. Thus, it is likely that the greatest information powers, such as China, the European Union, Russia and the United States, plus lesser

Enjoying this article?

- **Learn more about, discuss and collaborate on cyber security in the Knowledge Center.** *www.isaca.org/cybersecurity-topic*
- **Access career tools, resources and learn more about cyber security certifications on the CSX website.** *https://cybersecurity.isaca.org/*

powers such as Iraq and North Korea (all mentioned in the article), will continue to prepare for and possibly execute war-like activities in cyberspace, which is hardly a regional place.

My issues with the Valeriano-Maness argument do not diminish my respect for their scholarship. I believe that, were he alive today, Carl von Clausewitz, the Prussian general and military theorist, would say that "Cyberwar is the continuation of war by other means."[16]

Endnotes

1 Both Valeriano and Maness have moved on to other universities since the publication of their article.
2 Valeriano, B.; R. C. Maness; "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–11," *Journal of Peace Research*, May 2014, vol. 51, no. 3, p. 347-360, *http://jpr.sagepub.com/content/51/3/347.abstract*. The article and its accompanying database are available, but there is a fee of US $36 to download it.
3 *Ibid*., p. 3. Valeriano and Maness eschew the term "cyberattack" as they feel it "to be misguiding and inappropriate in that it conflates the tactic to sound something akin to a conventional military attack." With respect, I will use their terminology here.
4 *Ibid*., p. 5
5 I tried a few analyses of my own and found that I was not getting any new insights, so I stopped. The database is available along with the article.
6 *Op cit*, Valeriano and Maness, p. 3.
7 *Ibid*., p. 10
8 G7 2016 Ise-Shima Summit, "G7 Ise-Shima Leaders' Declaration," 26-27 May 2016, *www.mofa.go.jp/files/000160266.pdf*
9 Park, M.; D. Ford; "North Korea to U.S.: Show Evidence We Hacked Sony," CNN, 14 January 2015, *www.cnn.com/2015/01/13/asia/north-korea-sony-hack/*
10 Sanger, D. E.; E. Schmitt; "Spy Agency Consensus Grows That Russia Hacked D.N.C.," *The New York Times*, 26 July 2016, *www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html*

Brandon Valeriano, Ph.D., Replies

I am pleased to offer a response to Steven Ross's thoughtful review of our article; it is indeed an important topic for anyone concerned with cyberconflict. We cover the issue of the rate of attacks and what we call cyberpeace in our article "The Coming Cyberpeace."[17] While the rate is certainly increasing, there is no clear demonstration of severe attacks we might expect by now. Ukraine Black Energy was fixed fairly quickly by going to the substations. The recent US Democratic National Committee (DNC) and US Republican National Committee (RNC) hacks continue to show an absence of real information leaks[18] and the attacks on US electoral systems represent attempts, but no actual altering of electoral systems.[19] What we witness is cyberespionage, not cyberwar.

Interestingly, we were surprised by the relative lack of significant documented cyberincidents (hacking attempts and intrusions are, of course, fairly common). We assumed we would find more, but this has not been the case and continues to be the trend, in that we are locating only dozens per year. Our point is to counter language such as "could be," "possibly" or "in the future." We have a large amount of data on cyberactions being used in the last 20 years and see cyber as an additive power, not a sole method of attack. That cyber will be the method of first strike is conjecture, but, based on war gaming exercises, it is an unsure tactic that governments are not going to depend on when they attack. Plus, there is the issue of cyberactions being one-shot weapons. Once a vulnerability is exploited, the opposition will close that hole in the future. We are not in cyberwar and unlikely to ever see it. Thomas Rid, professor in Security Studies, King's College London (UK) writes frequently on this issue from the Clauzwitzian perspective.[20] What we are concerned about and fear in the future is government-led attacks on individuals such as activists, protestors and journalists.

Cyber used for violence and war is purely an additive technology, a method of espionage or disruption. Making this point clear is imperative as it shapes the policy we construct, our assumptions about future conflict, and can often exacerbate fears, making a technology with so many positive attributes closed to society.

11 Piiparinen, A.; "China's Secret Weapon in the South China Sea: Cyber Attacks," *The Diplomat*, 22 July 2016, *http://thediplomat.com/2016/07/chinas-secret-weapon-in-the-south-china-sea-cyber-attacks/*

12 *Bloomberg News*, "China Military Seeks to Bring Cyber Warfare Units Under One Roof," 22 October 2015

13 Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, 2013

14 Giles, K.; "'Information Troops'—A Russian Cyber Command?," 3rd International Conference on Cyber Conflict, 2011, *https://www.researchgate.net/publication/224247775_Information_Troops_-_A_Russian_Cyber_Command*

15 *Op cit*, Valeriano and Maness, p. 5

16 What he actually said is that "War is the continuation of politics by other means."

17 Valeriano, B.; R. C. Maness; "The Coming Cyberpeace: The Normative Argument Against Cyberwar," *Foreign Affairs*, 13 May 2015, *https://www.foreignaffairs.com/articles/2015-05-13/coming-cyberpeace*

18 Eichenwald, K.; "Dear Donald Trump and Vladimir Putin, I Am Not Sidney Blumenthal," *Newsweek*, 10 October 2016, w*ww.newsweek.com/vladimir-putin-sidney-blumenthal-hillary-clinton-donald-trump-benghazi-sputnik-508635*

19 Department of Homeland Security, Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security, press release, 7 October 2016, USA, *https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national*

20 Limnell, J.; T. Rid; "Is Cyberwar Real?," *Foreign Affairs*, March/April 2014, https:*//www.foreignaffairs.com/articles/global-commons/2014-02-12/cyberwar-real*