All That Which Is Old, Is New Again – Unlearned Lessons about Metrics of Success in Cyber

Harvey Rishikof

In September 2009, the ABA Standing Committee on Law and National Security, the National Strategy Forum, and the McCormick Foundation held a workshop assembling approximately 35 experts on national security threats in cyberspace. The 46-page report, *National Security Threats in Cyberspace*, explored the then cyber threat vectors, legal frameworks, organizational questions and what the future would bring, among other topics. Our reporter was Paul Rosenzweig; as always, he captured the essence of the discussion – and we ended the report with a chapter on the "Metrics for Success." In short, all that was old is new again – this report is almost 13 years old, but all the metrics remain relevant and the same, and sadly, to a great extent, the metrics reflect policies not met.

For the purposes of this discussion, I have reproduced Chapter 6 of the report in italics and made comments and responses in normal text.

> ***Metrics for Success***
>
> *The system today is in a crisis. That crisis is one that is only slowly becoming clear and achieving public awareness – but we stand at a crossroads.*
>
> *Today, determined adversaries can enter some classified systems undetected, encrypt data while in the systems, extract it, and leave behind autonomic tools that will dial back to the installer, over time, at a time of his or her programmatic choosing. That is an immensely serious concern. And if that can occur on classified systems, imagine what is happening in the unclassified domain.*

These are solely the opinions of the author and do not reflect the views, policies or thoughts of any private or government agency.

Harvey Rishikof is the Chair of the American Bar Association Standing Committee on Law and National Security Advisory Committee Chair. He is the former dean of the National War College in Washington, D.C., where he also chaired the department of national security strategy. Mr. Rishikof was a senior policy advisor to the Director of National Counterintelligence, ODNI, legal counsel for the deputy director of the Federal Bureau of Investigation, and dean of Roger Williams School of Law. Currently, he is also an advisor to the Harvard Law Journal on National Security and serves on the Board of Visitors at the National Intelligence University. He is also a Member of the National Academy of Sciences Commission on Law Enforcement and Intelligence Access to Plain Text Information in an Era of Widespread Strong Encryption: Options and Tradeoff. He recently co-authored The National Security Enterprise: Navigating the Labyrinth.

This statement remains true; we still are in crisis – see OPM hack, Microsoft Exchange, Solar Winds, Colonial Pipeline, Ransomware, etc. Nonetheless, this "crisis status" has continued since the last report. We have had some responses, like the public Stuxnet attack, for which no country takes credit, but by and large there have been few public responses to attacks in general and few consequences for our adversaries. The Biden Administration has made cyber a priority with the appointment of an excellent team, but the jury is still out on how effective they can be.

Most kinetic threats we will face can be thought about well in advance and can be prepared for. The cyberthreat will be executed in millisecond time with enduring consequences. If the Chinese military were at our borders ready to attack, we would deem that a crisis. Today, in the cyber domain, we are effectively at the same place. Questions remain:

- *How will we know when the crisis is over?*
- *How will we know if what we are doing is effective?*
- *How do we know if we've won?*
- *Or, put another way, given President Obama's commitment to the creation of a new "Cyber Czar" position within the White House, how will we know if the czar has succeeded?*

These are the fundamental structural questions for our system. One "czar" has come and gone, and yet based on the key fundamental questions we remain adrift. A new "czar" has been proposed by the latest NDAA of 2021 and has been appointed. Although an excellent choice, it remains unclear how effective the new Czar will be.

In asking these questions, we want to move away from traditional Washington metrics of success. By these standards, the czar will succeed if the staff and budget increase exponentially. The czar will be a real bureaucratic success if a fight with some in-house adversary is won.

And the czar will be a failure if some cyber-Pearl Harbor occurs on his watch and the czar is forced to resign.

Consequesntly, we have witnessed the OPM breach, Election hack of 2016, Solar Winds, No-Petya. Should I go on? Who has been held responsible, accountable, or fired?

None of these , of course, is a real measure of success. They assume a myopic "inside the Beltway" vision of reality in which only press releases count. Real success will be difficult to measure. We cannot, for example, say whether a reduction in the number of intrusions detected reflects our success in preventing them or a growing capacity on the part of the intruders to evade detection. Indeed, our only true measures of success are likely to be indirect ones that serve as proxies for our ultimate goal. Nevertheless, if we were to suggest some realistic measures by which our success over the next 4-8 years could be measured, the following would be a non-comprehensive list of metrics that ought to be considered:

Have we reduced the number of intrusions into American governmental systems?

- *What degree of success do NSA red teams have in penetrating our networks?*
- *Are we more effective at the attribution of malicious actors?*
- *Have we improved encryption standards?*
- *Does intrusion detection lead seamlessly to immunization and prevention, such that intrusions by a particular method are a one-time-only occurrence?*
- *Have we adopted an effective identity management system (more or less premised on the one outlined in Homeland Security Presidential Directive-12)?*
- *Is America more successful in offensive cyber intrusions than its opponents are (i.e., are America's offense and defense better than that of our opponents)?*
- *Have we enhanced coordination and agility in responding to events in a way that makes a Cyber Czar no longer necessary?*

This set of questions has answers that remain opaque and somewhat underwhelming– we are good at penetration but so are our adversaries; we are concerned that quantum physics will undermine encryption; attribution as the holy grail has improved but remains elusive; detections have not led to "seamless immunization and prevention"; we do not have an "effective identity management system"; the general consensus remains that offense beats defense; not only have we not solved the coordination problem but yet again in legislation we have called for a new "czar."

Has the private sector adopted appropriate security measures?

- *Have we increased the application of patches for vulnerabilities that are known to exist, where lethargy has delayed or prevented application?*

- *Are auditing schemes generally in place?*
- *Have they resulted in the adoption of generally accepted best practices that embody standards of care that the courts deem significant?*
- *Is private sector R&D increasing?*
- *Is there an appropriate liability regime in place that allows injured parties to seek compensation for consequential damage?*
- *Have we found ways to incentivize resiliency?*
- *Are we devising a more secure system architecture for the cyber domain? What are the prospects for its adoption and implementation?*

Again we have a disappointing set of responses to these questions; patches are faster as we move to the Cloud, but due to our movement to the widely adopted systems or clouds the ability to compromise trust has let to systemic attacks; the auditing schemes are not robust; the courts have not ventured into the space with much enthusiasm; R&D is increasing but the breadth of the attack surfaces have made the increase not meet the threat; again no, there has not been established a liability regime; again no, more calls for resiliency have been made but we have not used – tax codes, insurance premiums regulation, litigation or international treaties to reinforce a policy of resilience; we have launched for DIB companies a Cybersecurity Maturity Model Certification process but the role has been deeply problematic and the NIST/ISO framework has only gone so far.

Have we developed a doctrine of cyber warfare and response?

- *Do we know how we will respond to an overt cyber-attack that causes physical damage?*
- *Do we know what our response will be to a covert intrusion?*
- *Have we defined what constitutes an armed attack and when we will attribute that attack to a state actor?*
- *Has the law of armed conflict reached consensus on the definitions of lawful and unlawful use?*

Recently, U.S. Cyber Command (USCYBERCOM) announced its new doctrine of "Defend Forward" to generate effects in cyber against adversaries below the level of armed conflict, but it still is unclear what ultimate effect this new policy will have; the "grey space" or actions below the threshold of an armed conflict has become a cottage industry for the legal community of scholars but still remains open to debate; in short we have no shared consensus on "lawful and unlawful" use of cyber tools. There needs to be a proper forum to construct such a consensus; moreover, the tension between espionage and traditional military affairs or Title 10 v. Title 50 remains a continuing issue.

Have we improved international cooperation against cybercrime?

- *Are international requests for assistance routine and effective?*
- *Is information shared internationally quickly enough to have effect?*
- *Are the numbers of safe havens for cybercriminals being reduced?*
- *Is there international agreement on norms of behavior that have the effect of modifying the behavior of state actors?*

Although we have had some movement on international agreement regarding cybercrime, we still use as our domestic statue the Computer Fraud and Abuse Act of 2005 (18 USC 1030), since revised most recently in 2014; the process under the Mutual Legal Assistance Treaty (MLAT) remains notoriously slow and safe havens for cyber criminals remain; moreover, the UN Group of Governmental Experts process has grinded to a halt since major players such as China and Russia remain recalcitrant about the appropriate roles of international norms.

Have we internalized within the US government conceptions of cybersecurity that are currently lacking?

- *Does procurement policy take account of cyber vulnerabilities?*
- *Are there new federal acquisition rules that incorporate cybersecurity standards for all hardware?*
- *Does OMB fund cybersecurity projects adequately?*

As mentioned, we have launched for DIB companies a Cybersecurity Maturity Model Certification process, but the rollout has been deeply problematic and the NIST/ISO framework has gone only so far; the government's Einstein 1, 2. 3 cyber defense frameworks have not proven to be an effective defense; OMB neither has adequately funded nor overseen a regulated an effective defense for USG.

Have we taken leadership of the cyber issue?

- *Is there a national strategy in place that identifies roles and responsibilities throughout government and in the private sector? Is it a paper strategy or is it actually being implemented?*
- *Does the American public understand the scope and nature of the cyber problem?*
- *Do they care about it, and have they considered how cyber issues impact privacy and civil liberties?*
- *Have we changed the public's mindset on cybersecurity so that good practices are well accepted (much like wearing a seatbelt is now considered the norm)?*
- *Is more attention being paid to cyber conflict in the service academies?*
- *Has transparency increased, thereby enhancing public debate on the appropriate solution set?*

Although we have had the excellent Cyberspace Solarium Commission report (2021), and the commissioners have been effective in having several recommendations become part of the 2021 NDAA, it is unclear how the public views cyber security. There has not been an effective national strategy. Since 1997, we have had 13 cyber-related national strategies issued almost every two years, with three in 2018 alone. Most reports recommend the following reforms: better policies; better public-private practices; improved information-sharing; more centralized coordination and control; better practices for threat sharing of vulnerabilities; more agile and adaptable policies; legal reforms; improved training and education; more R&D; capacity building; and, the establishment and promotion of norms. In short, we have been saying and recommending the same solutions for last the 23 years. (see "From Solar Sunrise to Solar Winds: Two Decades of Cybersecurity Advice," by Michael Tanji). As an aside, during this period of time social media companies have revolutionized the information space and built a multi-billion-dollar market for personal digital data.

- *And the single key metric, which is almost immeasurable:*

HAVE WE EXERCISED VISIONARY AND COURAGEOUS POLITICAL LEADERSHIP TO FORMULATE A COHERENT POLICY?

No, though we have been admiring and writing about the problem for decades. The lessons about metrics remain unlearned. In short, we have yet to establish an effective policy and doctrine of deterrence for cyber. Hope springs eternal and all hope the Biden Administration will be successful where those before have failed.