

Lessons Learned
from the
2020
ICIT FALL BRIEFING
Secure Roadmap
for the Future

CYBERWARFARE

FEBRUARY 2021

THE ART OF CYBERWARFARE

How Military Doctrine Can Improve Communication, Collaboration and Coordination

Authored By:
Drew Spaniel, Lead Researcher, ICIT

Contributors:
Ok! Mek, Senior Advisor to the HHS CIO
and Technical Lead, Reimagine HHS

ICIT | Institute for Critical
Infrastructure Technology
The Cybersecurity Think Tank

DLT
A TECH DATA COMPANY

The Corona Virus pandemic disrupted the paradigm of workplaces, healthcare, the economy, and daily life. The transformational change was fast, and communication, coordination, and collaboration were essential for success in the tumult. At the October 2020 ICIT Fall Briefing: A Secure Roadmap for the Future, Oki Mek, the Lead Technical Integrator for Re-Imagine HHS, and Senior Adviser to the CIO, spoke about how he was able to increase the adoption of innovative and modern solutions within HHS to better deliver mission outcomes, improve service, and operate more efficiently. Mr. Mek focuses on initiating and leading change through digital transformation to enhance Americans' health and well-being through effective health and human services and fostering sound, sustained advances in the sciences underlying medicine, public health, and social services. Mr. Mek also teaches *Innovation in Cybersecurity* at the University of Maryland.

In his talk, Mr. Mek explained that America is woefully unprepared to secure its distributed control systems (DCS), supervisory control and data acquisition (SCADA) systems, supply chains, and other critical infrastructure against cyber threats. Each year in the United States, hundreds of millions of records are exposed in more than a thousand data breaches. The average cost of each enterprise security incident is around \$18 million, and experts anticipate that the aggregate cost of cybercrimes will exceed \$5 trillion over the next five years. To counter emerging unconventional, covert, and sophisticated threat campaigns, Mr. Mek believes that business, technology, and government leaders must adopt and interweave military-style strategies that align with their organizations' mission. To win these cyberspace battles, Mr. Mek derives lessons from Sun Tzu's book, *The Art of War*.

MILITARY STRATEGY 1: KNOW YOURSELF, KNOW THE ENEMY

Leaders such as Chief Security Officers (CSOs), must understand themselves, their personnel, their organization, and their adversaries to deploy an effective, proactive strategy. They should also understand the maturity of their organization's cybersecurity policies, processes, personnel, and mission-relevant technologies. Lastly, CSOs should consider how the organization's culture impacts security. Managing and measuring the workforce's knowledge, perceptions, assumptions, values, and attitudes towards cybersecurity empower CSOs to assess cultural adherence to security best practices and the potential for improvement.

Similarly, CSOs should recognize adversarial tactics and technologies. To secure an organization, it is vital to know how adversaries weaponize artificial intelligence, conduct social engineering, and evolve malware.

MILITARY STRATEGY 2: SPEED, FLEXIBILITY, AND ADAPTABILITY

Cyberwarfare is asymmetric and not bound by conventional warfare constraints such as force size, terrain complexity, or geopolitical ties. Instead, it is dictated by speed, flexibility, and adaptability. Unfortunately, some might characterize the Federal Government as the antithesis of those attributes. For example, over 95% of security, governance, risk, and compliance (GRC) processes are paper-based in federal systems. Other processes that are automated in the private sector, such as patching or continuous diagnostic and mitigation (CDM), are often manual in the public sector. In short, the government operates at a fraction of the pace of adversaries. Responding to a breach usually takes days, while discovering a security incident can take months or years.

However, CSOs can do better by adopting proactive technology that empowers their organizations to improve threat intelligence and cyber hunting. For instance, emerging technologies such as blockchain and artificial intelligence can increase the visibility, accountability, and transparency of security events and incidents, thereby allowing better analysis of adversaries' tactics, models, and tendencies.

MILITARY STRATEGY 3: SIMPLICITY

The complexity surrounding existing cybersecurity frameworks such as NIST, FedRAMP, and FISMA has led many Federal personnel to avoid institutionalizing security. Thus, CSOs and other leaders must find ways to improve compliance with their organization's cyber hygiene standards. To ensure this, they must measure, assess, and improve their cybersecurity maturity model so they can analyze the workforce and make strategic, targeting investments to elevate the workforce's understanding of security while also adopting solutions that make excellent cyber hygiene easy for the end-user.

CONCLUSION

Amidst the COVID-19 pandemic and the mass migration to telework environments, the Federal Government must improve the nation's critical infrastructure's cyber resiliency through proactive strategies such as those from *The Art of War*. Leaders must consider seriously how to embed security strategies, training, and awareness into their business, processes, and culture. Adversaries are agile, flexible, and adaptable; most federal systems are static and outdated. The disparity between emerging threats and the systems they are targeting is untenable. The Federal Government and other organizations must dispel the fears around understanding cybersecurity by teaching their personnel about the basic precautions necessary for cyber hygiene. In the words of moderator and ICIT Executive Director Joyce Hunter, "Cybersecurity is everybody's business, and it's the business of everybody."