Journal of Strategic Security

Volume 11 | Number 4 Article 5

The Cyber Threat and Globalization: The Impact on U.S. National and International Security. By Jack A. Jarmon and Pano Yannakogeorgos. Lanham, MD: Rowman & Littlefield, 2018.

Mark J. Roberts
Mideast Terrorism Analyst

pp. 85-88

Recommended Citation
Roberts, Mark J.. "*The Cyber Threat and Globalization: The Impact on U.S. National and International Security*. By Jack A. Jarmon and Pano Yannakogeorgos. Lanham, MD: Rowman & Littlefield, 2018.." *Journal of Strategic Security* 11, no. 4 (2019): : 85-88.
DOI: https://doi.org/10.5038/1944-0472.11.4.1716
Available at: https://scholarcommons.usf.edu/jss/vol11/iss4/5

***The Cyber Threat and Globalization: The Impact on U.S. National and International Security*. By Jack A. Jarmon and Pano Yannakogeorgos. Lanham, MD: Rowman & Littlefield, 2018. ISBN 978-1-5381-0431-6. Maps. Index. Notes. Sources cited. Tables. Text boxes. Pp. viii, 267. $39.00.**

The cyber realm touches every aspect of modern society. In a few years, business practices transitioned from manual typewriters to electric typewriters to word processors to supercomputers to iPhones. The cyber domain evolves and changes multiple times per day and embodies perpetual change. This constant state of change necessitates that modern cybernauts must actively learn and embrace change to remain relevant in ever-changing information tides.

The Cyber Threat and Globalization serves as a primer for the reader seeking to attain an understanding of cyber terminology and concepts. The authors bring impeccable credentials: Pano Yannakogeoros is Dean of Air University's Cyber College with past duties at Rutgers University and the United Nations Security Council; Jack A. Jarmon taught International Relations at the University of Pennsylvania, Seton Hall University, and Rutgers University. At Rutgers, he served as Associate Director of the Command, Control, and Interoperability Center for Advanced Data Analysis, which is a Center of Excellence of the Department of Homeland Security's Science and Technology Division.

The cyber domain encompasses the electromagnetic spectrum to house, transfer, and edit information via virtual networks and physical infrastructure. The national security community relied heavily upon computers during the Cold War. After the implosion of the Soviet empire, the cyber realm began to creep into non-governmental use. This led to quantum changes in electronics and technology, revolutionizing consumer products and industrial practices. As understanding and use of the Internet increased, the demand for data and bandwidth grew as well. This placed new demands upon an infrastructure that was itself burgeoning in an attempt to keep pace with markets that came into being overnight.

As more private and public sector entities came to rely upon this new capability, cybernauts became aware that massive quantities of data flying through wired and wireless systems needed increasingly sophisticated

levels of encryption and security to secure virtual and physical networks from hackers and corporate espionage. Cyber criminals and hackers posed threats of selling proprietary industrial information to competitors, using illicitly obtained information to conduct insider trading, and damaging a company from within through cyber sabotage revealing company secrets. This in turn led to new efforts to secure the networks.

These evolutions led to new advances in cryptology (use of mathematical algorithms and codes to protect information), a necessity as cyber attackers can be states (Russia, China, Iran), cyber criminals, and hackers. Attackers of all stripes engage in identity theft, corporate and industrial espionage, spear-phishing, introduction of malware, extortion, sabotage, and embezzlement. Attack agents sport myriad sophisticated techniques such as advanced cryptographic and cryptographic proficiency, comprehensive understanding of industrial control systems, dominance of numerous open and closed operating systems, and expert knowledge of telecommunications infrastructure.

The authors discuss and define the malware categories (viruses, bacteria, worms, denial of service attacks, distributed denial of service attacks, adware, spyware, botnets, rootkits, Trojan horse, flaws, logic bombs, backdoors, keyloggers, browser hackers, and ransomware) to better acquaint the reader with tools attacks use to ply their trade.

The explanation of the Internet and its various layers helps the reader understand the multiple strata involved. From the "Surface Web" through the "deep Web" and "Dark Web," the reader gains insights into private sites, blocked sites, unlinked sites, and non-HTML sites, to include structured and unstructured content. Although the Deep Web and Dark Web have nefarious facets, much of it is comprised of browsers who wish to remain anonymous. This anonymity is a source of frustration for law enforcement and international organizations. With the ever-changing currents of the cyber domain, international law governing it struggles to remain abreast of and relevant to it in attempts to construct enforcement mechanisms.

The globalization process further complicates efforts to stay ahead of developments in cyberspace due to real-time interdependence and interconnectedness. As a result, military and industrial technologies

https://scholarcommons.usf.edu/jss/vol11/iss4/5
DOI: https://doi.org/10.5038/1944-0472.11.4.1716

become more vulnerable to hostile actors and the United States faces new challenges in the cyber realm from China and a resurgent Russia. These factors also impact international and national policies, economies, and politics as information flows at the speed of light, shortening decision-making cycles and reaction times.

Cyberspace is a battlefield that has industrial control systems and critical infrastructure instead of combat aircraft, tanks, and military maritime vessels. As such, military adversaries, foreign intelligence services, terrorists, criminals, and disgruntled insiders can asymmetrically attack the power grid or main server to bring chaos and disarray to millions with one stroke of the keyboard. Due to the fluidity of the cyber dynamic, the policies of a company or government will continue to lag behind emerging and available technologies.

Then advent of social media has blurred the lines between governmental and industrial secrets, public discourse, private and personal affairs, personal opinions, news, and trivial information. Social media becomes a venue for advancing political agendas, propaganda, influencing public opinion, and personal aggrandizement. Governments, political parties, and corporations use contractors, troll farms, public relations firms and others to influence opinion, produce commentaries, and attempt to sway audiences worldwide.

Social media campaigns were integral to the Arab Spring of 2011, and to recent U.S political campaigns. The use of Facebook, Twitter, Snapchat, and Instagram can help enhance situational awareness or galvanize a mob in a short time. Social media also poses operational security dilemmas for those working in security. There have been numerous examples of security and intelligence personnel who injudiciously posted their occupations on various social media platforms, degrading their effectiveness and the mission of their agency.

The authors provide useful insights how Russia, China, extremists, and terrorists exploit the cyber domain to conduct economic and industrial espionage, information and propaganda operations, recruiting initiatives, and radicalization campaigns. Cyber innovations also open up new opportunities for public-private partnerships to enhance economic initiatives and promote better efficiencies in governmental affairs.

The Cyber Threat and Globalization is a solid primer for those seeking to understand basic concepts and how they fit into the national security of the United States. It is a useful tome for quick reference.

Mark J. Roberts, Mid-East Terrorism Analyst

https://scholarcommons.usf.edu/jss/vol11/iss4/5
DOI: https://doi.org/10.5038/1944-0472.11.4.1716