2022

Faces of NPS: Capt. Scott Jasper, PhD (Ret)

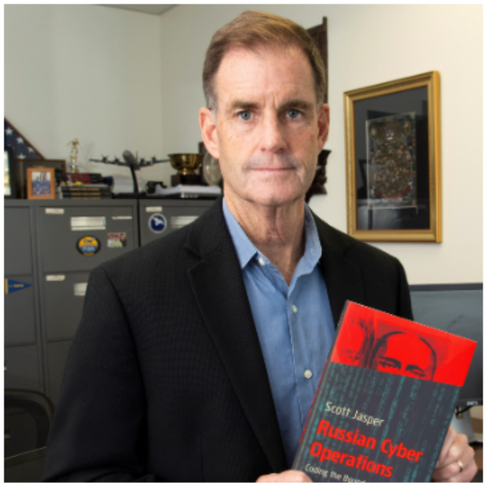
Jasper, Scott

Monterey, California, Naval Postgraduate School Foundation

https://hdl.handle.net/10945/71191

Faces of NPS

Spotlighting the students, faculty, staff and alumni of our Nation's premier defense education and research institution.



Capt. Scott Jasper, PhD (Ret)

SENIOR LECTURER, NATIONAL SECURITY AFFAIRS DEPARTMENT
CAPT, USN (RET)

Capt. Scott Jasper, PhD (Ret):

Retired U.S. Navy Captain Scott Jasper is a Senior Lecturer at the National Security Affairs Department at the Naval Postgraduate School, specializing in defense strategy, hybrid warfare, and cyber policy. He received his Ph.D. from the University of Reading, U.K. He is the author of Russian Cyber Operations: Coding the Boundaries of Conflict (Georgetown University Press), Strategic Cyber Deterrence: The Active Cyber Defense Option (Rowman and Littlefield) and editor of Conflict and Cooperation in the Global Commons, Securing Freedom in the Global Commons, and Transforming Defense Capabilities: New Approaches for International Security. Scott has published chapters in various handbooks related to cybersecurity and articles in Strategic Studies Quarterly, Signal Magazine, United States Cybersecurity Magazine, the International Journal of Intelligence and CounterIntelligence, The National Interest, Small Wars Journal, and The Diplomat, and blog posts for The Conversation, the Atlantic Council, The Foreign Policy Research Institute, and Council on Foreign Relations. He has spoken on defense and cyber issues on national media outlets, like NPR, KCBS Radio SF, and The First TV, and provided commentary in international newspapers, such as The Los Angeles Times, Daily Express UK, French daily Libération, and S&P Global Market Intelligence.

> *"The formulation of U.S. responses to strategic competitor cyber operations requires a thorough understanding of geopolitical ramifications. Students should understand how they embrace technical innovation and operational doctrine. The defeat of their ambitions will take an aggressive approach that combines technical solutions for resilience with national-level methods for cost imposition."*

Your publications, specifically your book Russian Cyber Operations: Coding the Boundaries of Conflict, offer the national security community a plan of action to defend against Russian cyber campaigns. What is the most important or immediate action that the DOD can take to better protect the U.S. from cyber threats?

My publications stress the need to adopt cloud-centric cyber defense capabilities. For reference, a Joint Cybersecurity Advisory released in April 2022 on Russian State-Sponsored and Criminal Cyber Threats to Criminal Infrastructure recommends use of endpoint detection and response (EDR) tools to identify, detect and investigate abnormal activity. AI-powered versions of those devices using models created in Machine Learning environments can prevent weaponized files and malicious scripts. For example, the BlackCat ransomware group, linked to Russian-based DarkSide that attacked Colonial Pipeline a year ago, leverages PowerShell and Batch scripts to deploy ransomware and compromise additional hosts.

Disinformation is a key component of what's become known as "hybrid" warfare, and Russia is no stranger to using disinformation alongside state-sponsored cyberattacks on critical infrastructure in Western countries (energy, elections, banks, etc.). In your opinion, which cyberthreats would have the most catastrophic effect on our national security?

Russia has used disinformation on social media to sow discord and divide our society in recent elections. Their cyber units in the 2020 Presidential election did not repeat the hack and leak pattern seen four years prior. Instead, Russia stole information useful for foreign policy interests. Yet more concerning for national security was the SolarWinds campaign by the Russian Foreign Intelligence Service revealed the month after the election. They compromised the global technology supply chain to infect roughly eighteen thousand SolarWind customers with malware. The threat posed a grave risk to the federal government, critical infrastructure entities and private sector organizations.

As an expert in national security, you recognize the strategic implications of emerging technologies such as AI, cloud computing, etc. With cyberspace becoming one of the dominant battlespaces of the future, how do you see these technologies supporting offensive cyber operations? What are some of the geopolitical implications of using these technologies to support DOD capabilities?

Researchers have illustrated how AI technologies can enhance cyber operations along every step of the attack sequence, to include in the MITRE ATT&CK framework recognized by the federal government and cybersecurity industry.   Russia and China have prioritized so far, the use of AI technologies in their aerial, ground, and maritime weapon systems for potential autonomous operations. While the US DOD Responsible AI Strategy emphasizes the mandate to design AI capabilities to fulfill intended functions, with the ability to detect and avoid unintended consequences.

Our strategic competitors are attempting to use their technological capacity and geopolitical influence to reshape the international order. From Russia's invasion of Ukraine to China's Belt and Road Initiative, we appear to stand at an inflection point.
a. What might be at stake if the Department of Defense does not innovate or adopt new technologies rapidly enough for a future multi-domain battlefront?

Concur that strategic competitors continue to challenge or violate the rules-based international order. The innovation and adoption of new technologies by the Department of Defense, such as in our own hypersonic weapons, are necessary to deter these competitors from engaging in activity that would draw the United States into direct conflict.

b. How can NPS better support collaboration with private industry to rapidly equip the DOD and our warfighters with the best and most relevant technologies?

The use of a CRADA (Cooperative Research and Development Agreement) is a great way to collaborate with industry. NPS recently announced a CRADA with Microsoft Corporation. I used a CRADA with Palo Alto Networks to explore the sufficiency of cloud-centric cyber defense capabilities to detect advance threats.

How did your own time in the military inform how you educate current operational students? What do you believe is the most critical takeaway for those who attend NPS?

With my students, I stress innovation in warfighting domains to counter demonstrated and documented advances or attacks by our adversaries.
The most critical takeaway is a mindset to adapt to changing operational circumstances.

At NPS, you educate future military leaders, some of whom will become decision-makers in national security policy and defense strategy. How do you approach educating these students, knowing that future challenges are ever evolving and unpredictable?

I teach analytical frameworks, such as the technical and legal framework in my Russian Cyber Operations: Coding the Boundaries of Conflict book that is enduring in value to understand how Russian cyber operations function in forms of conflict and competition.

Why is it important for NPS students in cyber operations or cyber systems programs to also understand national security affairs?

The formulation of U.S. responses to strategic competitor cyber operations requires a thorough understanding of geopolitical ramifications. Students should understand how they embrace technical innovation and operational doctrine.

The defeat of their ambitions will take an aggressive approach that combines technical solutions for resilience with national-level methods for cost imposition.

https://www.npsfoundation.org/faces-of-nps/scott-jasper