JUNE 2023

GUARDIANS OF THE VIRTUAL FRONTIERS:

Unleashing the Power of Offensive Cybersecurity Operations

Authored By:
Dustin Sachs, Director of Research and Content Strategy, ICIT

Contributors:
Pete Slade, ICIT Fellow

Stan Mierzwa, ICIT Fellow

Malcolm Harkins, ICIT Fellow

ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

Guardians of the Virtual Frontiers: Unleashing the Power of Offensive Cybersecurity Operations

June 2023

ICIT would like to thank the following experts for their contributions to this paper:

- Dustin Sachs, ICIT Director of Research and Content Strategy
- Pete Slade, ICIT Fellow
- Stan Mierzwa, ICIT Fellow
- Malcolm Harkins, ICIT Fellow

Contents

Introduction

Offensive security operations are essential in combating cyber threats and ensuring the safety and security of the United States' digital landscape. Historically, the responsibility for offensive cyber-related attacks has rested with military outfits due to the nature of the country's democratic values and approaches. However, the growing prevalence of cyber-attacks and the potential risks associated with them necessitate a reevaluation of offensive security strategies. This article explores the potential risks of offensive cybersecurity operations, the need for the United States government's involvement, and how ethical conduct and adherence to international law can be ensured. It also discusses specific technologies, strategies, and collaborations that should be prioritized to combat cyber threats effectively.

Background on FY2024 US Cyber Command Request

US Cyber Command (USCYBERCOM) has requested $89.4 million for the Joint Common Access Platform (JCAP) in fiscal year 2024. The JCAP is a key offensive cyber platform allowing USCYBERCOM to connect to its targets beyond friendly firewalls. The platform was previously classified in budget documents, but the funding request provides rare insight into a previously undisclosed program.

ManTech, a Virginia-based information technology company, is developing the JCAP. The company was awarded a $265 million contract in 2020 to support the program over three-and-a-half years. The platform is expected to be completed in fiscal year 2024.

The JCAP will provide USCYBERCOM with several capabilities that are currently unavailable. These include the ability to:

- Conduct offensive cyber operations against enemy targets
- Protect US networks from cyberattacks
- Conduct cyber intelligence gathering and analysis
- Train and prepare cyber operators

The JCAP is a significant investment in USCYBERCOM's offensive cyber capabilities. The platform will allow the command to conduct more effective and targeted cyberattacks against enemy targets. The JCAP will also help to protect US networks from cyberattacks and improve the command's ability to gather and analyze cyber intelligence.

The development of the JCAP is a sign of the growing importance of cyber warfare. Cyber attacks become a more common and dangerous threat as the world becomes increasingly interconnected. The JCAP will help to ensure that USCYBERCOM is prepared to meet this threat.

In addition to the JCAP, USCYBERCOM has requested funding for several other cyber programs in Fiscal Year 2024. These include:

- The Joint Cyber Warfighting Architecture (JCWA), which is the command's overarching architecture for conducting cyber operations

- The Cyber Mission Force, which is the command's workforce of cyber operators
- The Cyber National Mission Force, which is a joint task force that conducts cyber operations in support of other military commands

The funding request for these programs reflects the growing importance of cyber warfare to the US military. Cyber-attacks become a more common and dangerous threat as the world becomes increasingly interconnected. The US military invests heavily in cyber capabilities to ensure it is prepared to meet this threat.

Collaboration to Combat Cyber Threats

Collaboration between the US Cyber Command, other government agencies, and private-sector partners is critical and achievable through information sharing and coordinated incident response. In the digital age, all organizations, especially essential infrastructure entities, are easily accessible and susceptible to attacks by foreign nations. By sharing threat intelligence and coordinating response efforts, organizations can improve their abilities to detect and respond to cyber-attacks, mitigating their impact on systems and infrastructure and playing their part in national defense.

Potential Risks

Any time offensive cybersecurity operations are deployed, they carry risks. One such risk is the potential for escalation, as operations, when attributed, may bring a retaliatory response from the adversary, leading to a continued escalation through a cycle of attacks and counterattacks. Another risk is collateral damage, as offensive operations can have unintended consequences, such as disrupting systems and networks that are not the intended targets but fall within the digital blast radius. These unintended impacts can result in long-term economic or social consequences.

Offensive operations can spiral out of control without proper checks and evaluation, leading to a larger conflict or war. Oversight is necessary to assess potential consequences, weigh responses against the risk and rewards of conducting an operation, and ensure timely decision-making without unnecessary bureaucracy.

Attribution is another significant issue in offensive cyber warfare. It is challenging to attribute a cyber-attack to a specific actor or group with certainty, and false flag operations further complicate the process. Once attribution is assigned (correctly or incorrectly), it can have significant diplomatic and political consequences, such as loss of trust between nations and the potential for further offensive operations by wrongfully accused parties.

Offensive Security by Private Entities

Engaging in offensive cybersecurity operations poses legal and ethical dilemmas that private organizations may struggle to navigate. Such operations can potentially violate national and international laws, raising concerns about ethics and compliance. The absence of a unified legal framework creates uncertainty, compromising global security and escalating cyber conflicts. Moreover, private organizations may inadvertently provoke retaliation from both state and non-state actors,

leading to an escalation of attacks that undermines the stability of critical infrastructure and puts civilian targets at risk.

Private organizations conducting offensive cybersecurity operations often lack the oversight and transparency that government agencies are subjected to. This absence of scrutiny can compromise accountability, as there may be limited mechanisms in place to ensure compliance with ethical standards, international norms, and human rights. Moreover, private entities may lack the expertise and protocols to anticipate and mitigate risks effectively. Collateral damage to innocent parties or inadvertent disclosure of sensitive information can result in severe reputational damage for the involved private organization, eroding public trust and potentially leading to legal consequences.

Ensuring Ethical Conduct and Adherence to International Law

Adjustments to regulations and rules are necessary to ensure ethical conduct and adherence to international law. Existing regulations primarily focus on cybersecurity defense and prevention, but offensive measures require different considerations. Collaboration with organizations like INTERPOL, with expertise in secure information sharing and international law enforcement, can provide insights into proper adherence to international law and practices.

The recently enacted Cyber Incident Reporting for Critical Infrastructure Act of 2022 can also play a crucial role. By aligning offensive operations with the Act, proper situational awareness can be achieved, enhancing the effectiveness of offensive operations targeting specific threats.

Impact of Increased Funding on the Cybersecurity Landscape

Increased funding can have a transformative impact on the overall cybersecurity landscape. It can support larger-scale research efforts, focusing on offensive cybersecurity attacks to deter future attacks. Robust research can provide a deeper understanding of the current threat landscape, effective response strategies, and the potential consequences of offensive operations. This knowledge can shape policies, improve defensive capabilities, and strengthen the United States overall cybersecurity posture.

Collaboration with Government Agencies and Private Sector Partners

Combating cyber threats requires collaboration between the US Cyber Command, other government agencies, and private-sector partners. Collaborating with organizations like INTERPOL and InfraGard, which prioritize collaboration and possess expertise in cybersecurity and critical infrastructure defense, can foster mutual understanding and improve joint efforts. Public-private partnerships can facilitate information exchange, collaborative research, development, and effective cybersecurity measures.

Conclusion

Offensive security operations are crucial in today's increasingly digital world. The United States government's involvement in these operations is necessary to address the growing risks and challenges associated with cyber-attacks. Collaboration between the US Cyber Command, government agencies, and private-sector partners is essential for effective cybersecurity defense. Proper evaluation, oversight, and adherence to international law can mitigate the potential risks of offensive operations. Increased funding can drive research efforts, shape offensive strategies, and strengthen the overall cybersecurity

landscape. By working together, we can protect critical infrastructure, safeguard national security, and ensure a secure digital future for the United States.

About the Organization

The Institute for Critical Infrastructure Technology (ICIT) is the nation's leading cybersecurity think tank providing **objective, nonpartisan research, advisory,** and **education** to **legislative**, commercial, and public-sector cybersecurity stakeholders.

ICIT understands that only through generative and focused collaboration will cybersecurity and national security communities make the quantum leaps necessary to defend against today's hyper-evolving adversaries. In response, we facilitate a robust platform of programs, knowledge sharing, cutting-edge research, and publications that support the exchange of ideas and provide a forum for cybersecurity leaders to engage in the meaningful discourse needed to effectively support and protect our nation's critical infrastructures.

References

Borghard, E. D., & Lonergan, S. W. (2019). Cyber Operations as Imperfect Tools of Escalation. *Strategic Studies Quarterly*, *13*(3), 122–145. https://www.jstor.org/stable/26760131

IC3.GOV. (2021). Internet Crime Report 2020. Retrieved from: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

INTERPOL. (2023). INTERPOL Member Countries. As retrieved on April 23, 2023, from: https://www.interpol.int/Who-we-are/Member-countries

Mierzwa, S. J., Drylie, J. J., Ho, C., Bogdan, D., & Watson, K. (2022). Ransomware Incident Preparations with Ethical Considerations and Command System Framework Proposal. Journal of Leadership, Accountability and Ethics, 19(2). https://doi.org/10.33423/jlae.v19i2.5112

Mierzwa, S., Spath-Caviglia, L. & Christov, I. (2021). Commentary or Perspective: Opportunities to Leverage the Use of Global Public Health Innovative Research Technology in Combatting Cybercrime. Journal of Leadership, Accountability and Ethics. 18(4). https://doi.org/10.33423/jlae.v18i4.4608

Mierzwa, S., RamaRao, S., Jung Ah, Y., Gyo, B. (2020). Proposal for the Developing and Addition of a Cybersecurity Assessment Section into Technology Involving Global Public Health. International Journal of Cybersecurity Intelligence & Cybercrime. 3(2). https://www.doi.org/10.52306/03020420BABW2272

Pancevski, B. & Katz, B. (2023). Hack Fails to Halt Plans in Europe. The Wall Street Journal. Saturday/Sunday, April 22-23, 2023. A11.

Pomerleau, M. (2023, April 12). *US Cyber Command requests nearly $90m for offensive platform*. DefenseScoop. https://defensescoop.com/2023/04/12/us-cyber-command-requests-nearly-90m-for-offensive-platform/

Willett, M. (2022). The Cyber Dimension of the Russia-Ukraine War. Survival. 64(5). https://doi.org/10.1080/00396338.2022.2126193