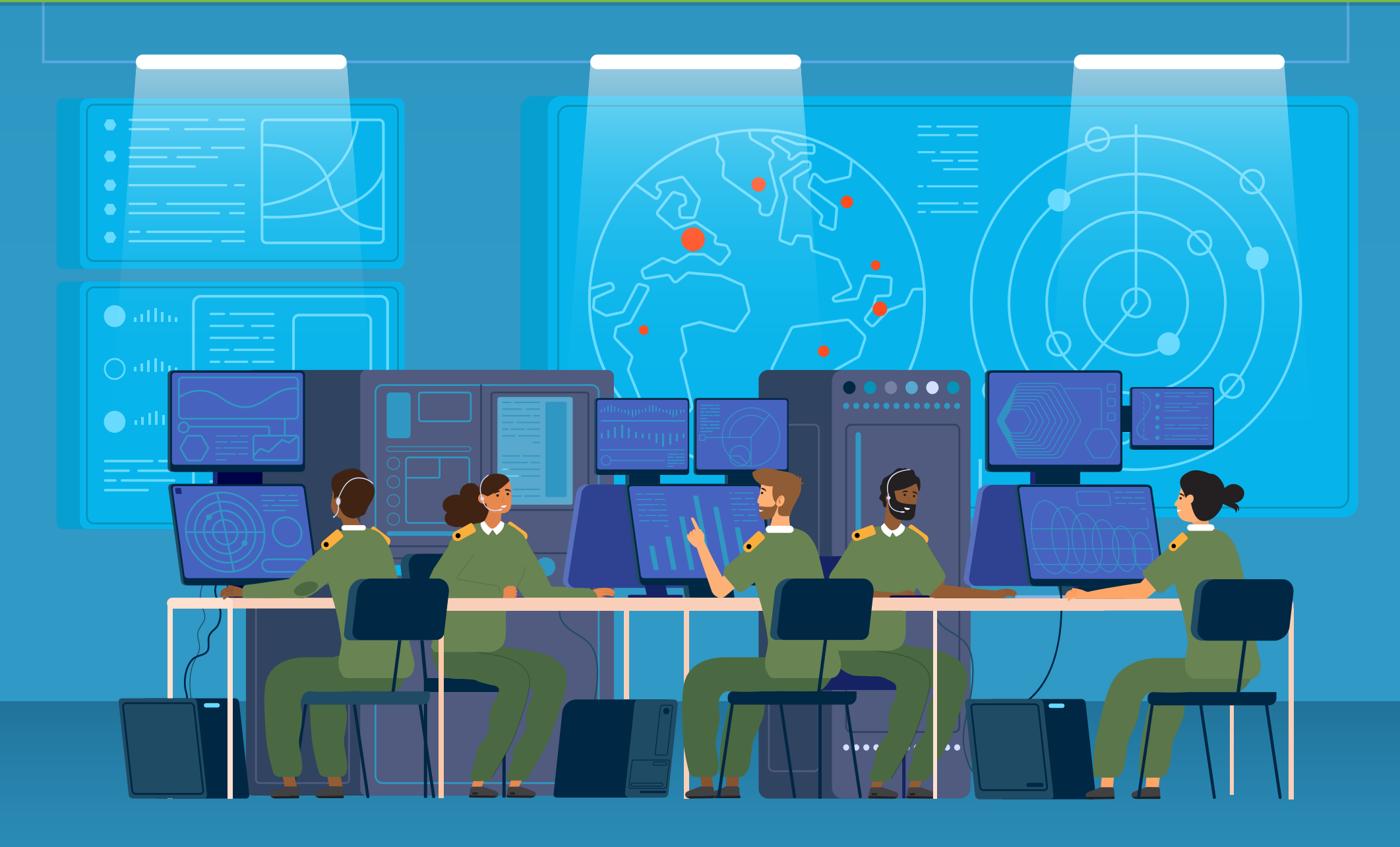
HANDLING CYBER CONFLICT IN MILITARY OPERATIONS



Cyber threats put U.S. national security at risk. The widespread impact of cyber conflict ranges from damage to critical infrastructure to the disruption of military operations. As cyber warfare becomes more sophisticated, the military relies on innovative techniques and collaborative approaches to protect national security.

CYBER THREATS AGAINST THE US

The U.S. is one of the largest targets for cyberattacks. In 2023, a total of 46% of global ransomware attacks targeted the U.S.

> "I would tell you that we're under attack every day in the cyber domain and the information space."
>
> *— Gen. Glen D. VanHerck, Air Force Commander, United States Northern Command (USNORTHCOM) and North American Aerospace Defense Command (NORAD)*

CYBER THREATS TO NATIONAL SECURITY

The top threats to national security include cyber espionage and sabotage. U.S. cybersecurity priorities focus on the following threats:

Advanced Persistent Threats: APTs are adversaries that conduct ongoing attacks meant to disrupt networks, steal data and infiltrate military or government organizations.

Cyber Espionage: Enemy actors use cyberattacks to spy on the U.S. military and government. Spyware, phishing attacks and other types of attacks can breach secure networks and put sensitive information at risk.

Cyber Sabotage: Attackers use cyber sabotage to disrupt or weaken targets. For example, malware can corrupt networks and weaken national security.

Cyber Psychological Warfare: Cyberattacks that spread disinformation and propaganda can have a significant impact on national security, influencing the outcome of elections and eroding trust in the media.

TYPES OF CYBER WARFARE ATTACKS

Cyberattacks take many forms, from phishing attacks designed to steal personal identifying information (PIN) to malicious software that infects computers. In the cyber warfare arena, the most common types of attacks include the following:

Malware: Attackers use malware to gain access to secure networks and information. Spyware, for example, can monitor activity and steal sensitive data.

Ransomware: By encrypting confidential data and holding it for ransom, attackers can disrupt operations and fund future attacks.

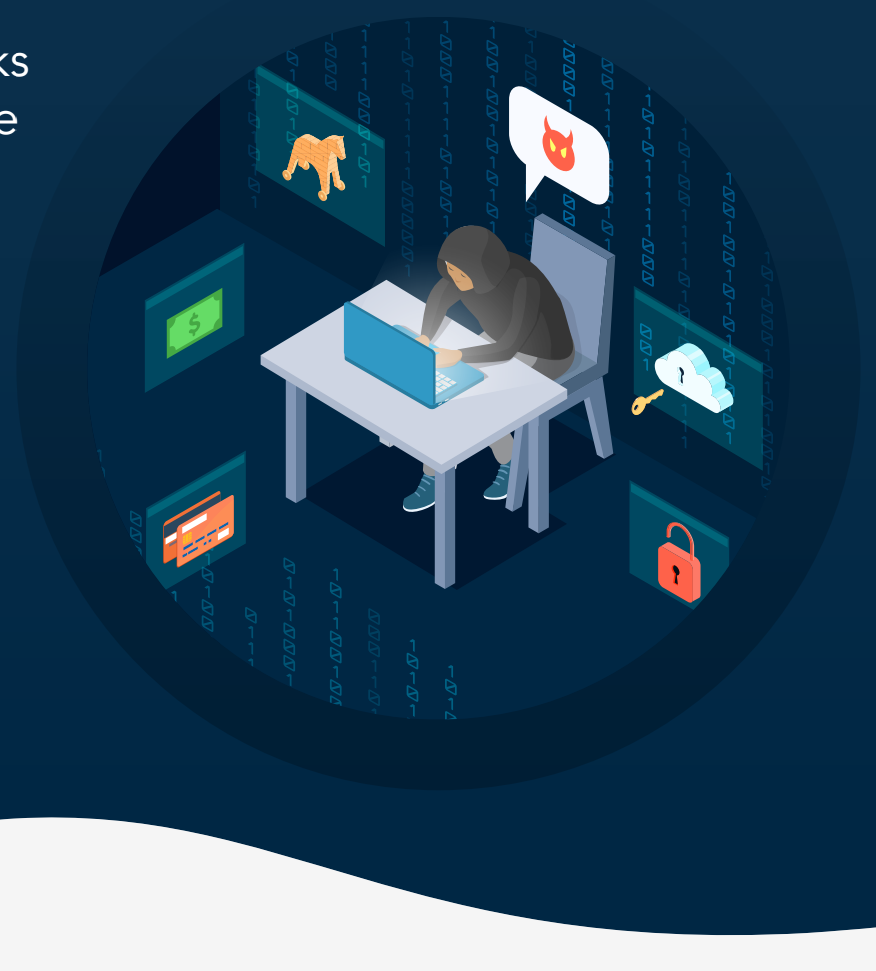
Distributed Denial of Service Attacks: DDoS attacks disrupt networks by overwhelming them with fake requests. This can block access or disrupt systems.

WHO ARE THE CYBERATTACKERS?

Armed conflict can look very different from cyber conflict. Cyberattackers can be state actors, cyber mercenaries or other malicious groups.

State Actors: Government-sponsored cyberattacks have grown more sophisticated. The following are five countries that are capable of large-scale cyber war:

- China
- Russia
- Iran
- United States
- North Korea



Cyber Mercenaries: Hacker groups, driven by profit, sell their services and spyware to state actors.

Cyber Terrorists: Twenty-first century terrorist organizations engage in cyber terrorism to incite fear and harm national security.

Hacktivists: Hackers seeking to effect social change can play a role in cyber warfare. For example, in 2022, several hacktivist organizations declared war against Russia after its invasion of Ukraine.

CYBER CONFLICTS IN THE 21ST CENTURY

Cyber conflict puts the country at risk. Even attacks that aren't directly targeted at the government can have major national security implications. The impacts of cyber warfare include the following:

Critical Infrastructure Disruptions: Attacks targeting infrastructure such as the country's electrical grid can cause physical and economic damage.

Data Breaches: Hacking that compromises classified information can disrupt operations and expose the country to future attacks.

Military Sabotage: Cyberattacks that target military operations or infrastructure can affect military readiness.

Cyber operations have grown increasingly sophisticated in the past two decades. Around the world, government organizations have faced significant disruption due to cyberattacks.

CYBER WARFARE TIMELINE

2003: Cyberattacks breach the U.S. Department of State and the U.S. Department of Homeland Security (DHS) in a suspected Chinese state-sponsored act of cyber warfare.

2007: Estonia experiences a DDoS attack that crashes government networks. Political tensions with Russia likely motivated the attack.

2009: Over 100 countries report targeted hackings in the GhostNet attack, which extracted confidential information as part of a cyber espionage network.

2010: Operation Olympic Games sabotages Iran's nuclear program using a computer worm. The U.S. and Israel likely collaborated on the cyberattack.

2016: U.S. Cyber Command targets the Islamic State group in Operation Glowing Symphony, an operation that disrupted the terrorist organization's cyber operations.

2021: The Colonial Pipeline ransomware attack disrupts critical infrastructure in the U.S., revealing how cyber risks can quickly become a national security issue.

2022: Russian cyberattacks target Ukraine, while hacktivists, including Anonymous, declare war on Russia.

2023: Hacktivists target NATO and steal 3,000 documents.

In the U.S., persistent attacks have targeted the Pentagon, the defense industrial base (DIB) and other U.S. Department of Defense (DOD) targets. From 2015 to 2021, DOD reported more than 12,000 cyber incidents.

COMBATING CYBER CONFLICT FOR NATIONAL SECURITY

U.S. cyber operations take defensive and offensive approaches to protecting national security.

U.S. NATIONAL CYBERSECURITY TEAM

U.S. Cyber Command: As part of the Defense Department, USCYBERCOM coordinates cyberspace operations. The cyber military organization includes the U.S. Army Cyber Command, U.S. Fleet Cyber Command and U.S. Marine Corps Forces Cyberspace Command.

NSA Cybersecurity: The National Security Agency operates a cybersecurity division tasked with preventing threats to national security systems.

Cybersecurity and Infrastructure Security Agency: Part of the DHS, CISA protects federal networks and coordinates critical infrastructure security.

DEFENSIVE CYBERSPACE OPERATIONS

Defensive cyberspace operations (DCO) protect U.S. networks and systems. They also monitor threats and conduct vulnerability assessments.

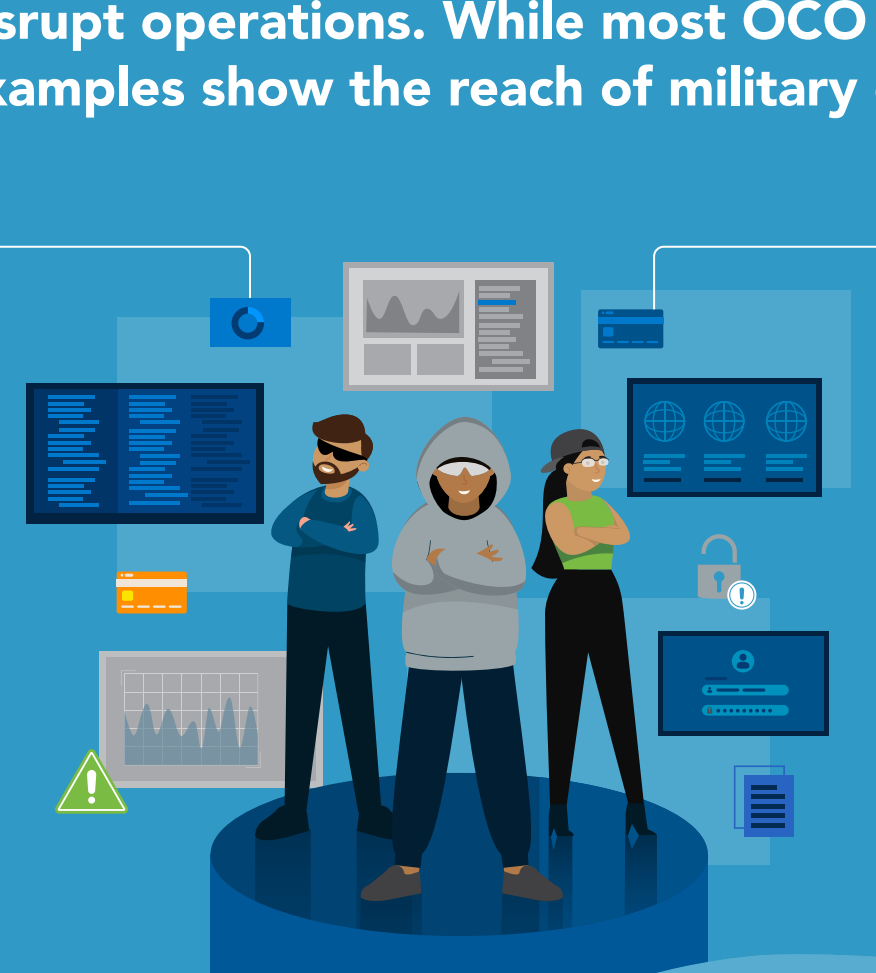
2023 DOD Cyber Strategy: A top Defense Department priority will focus on defensive operations to protect the DOD Information Network.

Protecting the DIB: The military uses cyber operations to protect the DIB, which develops and manufactures defense technologies.

OFFENSIVE CYBERSPACE OPERATIONS

Offensive cyberspace operations (OCO) target hostile organizations, collect intelligence and disrupt operations. While most OCO missions are highly classified, two examples show the reach of military cyber operations.

Operation Olympic Games (2010): In a targeted cyberattack, the Stuxnet computer worm destroyed nearly 1,000 uranium enrichment centrifuges at an Iranian nuclear fuel processing facility. While the U.S. hasn't officially claimed responsibility for the operation, it significantly hampered Iran's nuclear program.



Operation Glowing Symphony (2016): In the "most complex offensive cyberspace operation USCYBERCOM has conducted to date," the Defense Department infiltrated the Islamic State group's networks and significantly disrupted the terrorist organization's operations.

CONCLUSION

Cybersecurity professionals in the military use cutting-edge techniques to fight cyber conflicts. Maintaining security requires sophisticated tools and coordinated efforts. As events such as the Colonial Pipeline attack reveal, the nation's security depends on cybersecurity.

augusta.edu/online/ms-information-security-management.php

AUGUSTA UNIVERSITY ONLINE

Sources:
https://www.cybercom.mil/
https://www.nsa.gov/Cybersecurity/
https://www.cfr.org/cyber-operations/titan-rain
https://www.gao.gov/products/gao-23-105084
https://cybermagazine.com/articles/getac-experts-reveal
https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis
https://www.a10networks.com/blog/top-cyber-war-techniques-and-technologies/
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF
https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats-and-nation-state-actors
https://www.reuters.com/technology/alliance-40-countries-vow-not-pay-ransom-cybercriminals-us-says-2023-10-31/
https://www.defense.gov/News/News-Stories/Article/Article/3322765/cyber-command-nsa-successes-point-way-to-future/
https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years
https://www.defense.gov/News/News-Stories/Article/Article/3553150/emerging-threats-are-shaping-future-of-homeland-defense/
https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony
https://www.americanbar.org/groups/law_national_security/publications/aba-standing-committee-on-law-and-national-security-60-th-anniversary-an-anthology/cyber-conflict-from-apathy-to-action/