OSINT Collection Plan to Address National Security in Cyberspace

By: Adam Mohmoud
BLHV 2300 Introduction to Applied Intelligence
Dr. Frederic Lemieux

Objective: This topic aims to examine the escalating threat of cyberattacks originating from state-actors, analyzing their tactics, motivations, and potential consequences for national security. Additionally, it explores how robust defense frameworks, coupled with open-source intelligence (OSINT), can enhance cybersecurity resilience, facilitate threat detection, and strengthen national security strategies against emerging cyber threats.

Background: Cybersecurity has become a defining challenge for national security, as digital threats from state-sponsored groups and independent cybercriminals continue to evolve in sophistication and scale. State actors often engage in cyber warfare, espionage, and critical infrastructure attacks to undermine national stability, while non-state actors including hacktivists, cybercriminal organizations, and terrorist networks leverage cyberattacks for financial gain, ideological influence, or disruption. Governments and intelligence agencies must implement advanced defense frameworks to counter these threats, integrating proactive cybersecurity measures and real-time intelligence gathering. Open-source intelligence (OSINT) plays a pivotal role in this effort, enabling analysts to monitor emerging cyber threats, identify adversary tactics, and anticipate potential vulnerabilities.

Relevance: By exploring the interplay between cyber threats, national security defense mechanisms, and OSINT-driven intelligence, this topic provides a strategic foundation for mitigating cyber risks, strengthening resilience, and ensuring national stability in an era of digital warfare.

Source	Type of Sources (1)	Tools and Technologies (2)	Timeline (3)	Potential Challenges (4)	Provide complete reference of sources (APA / URL, etc.)
MITRE Att&ck Framework	Public Records	A knowledgebase source that provides a comprehensive guide for understanding cyber tactics, techniques, and procedures (TTP). This includes understanding adversary behavior and mapping a critical infrastructure that can be targeted.	05/27/2025 – 05/28/2025	The Att&ck tool is valuable, but it does not address all threats to national security. Due to the constant evolution of the threat landscape, the framework is constantly updated which would require trained experts in threat intelligence to guide you through this entire framework.	https://attack.mitre.org/
NIST Framework NIST-SP-800-171	Public Records	A risk-based framework that offers a structured approach through five core functions: **Identify, Protect, Detect,**	05/27/2025 – 05/28/2025	NIST's framework focuses on structured cybersecurity policies and best practices, but it does	https://www.nist.gov/cyber framework

		Respond, and Recover. Various tools and technologies align with these functions to enhance security operations.		not provide real-time threat intelligence. National security requires continuous monitoring and adaptive threat detection.	
Cyber Kill Chain Model	Public Record	A widely used framework for analyzing cyberattacks. It outlines **seven attack stages** - Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control (C2), and Actions on Objectives.	5/27/2025-05/28/2025	The Kill Chain is a retrospective model, meaning it analyzes attack phases after an incident occurs, rather than providing real-time defensive actions. The Cyber Kill Chain does not fully account for modern threats.	https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
"Significant Cyber Incidents" By: Center For Strategic & International Studies (CSIS)	Media Source	Google as a research tool. The CSIS website provides a most up-to-date timeline of significant cyber incidents from both state and non-state threat actors.	05/30/2025 – 05/31/2025	OSINT sources often present fragmented or unreliable data, leading to inconsistencies that complicate the validation of cyber incident timelines. The dynamic nature of cyber threats, coupled with the	https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

				potential for misinformation and gaps in reporting, makes it challenging to construct an accurate chronological sequence of events, requiring cross-referencing and advanced analytical methods to ensure credibility.	
‘72% of cyber leaders say risks are rising. Here's how states and businesses are responding’ By: The World Economic Forum	Media Source	Google as a research tool. The World Economic Forum press release based on research conducted by Harvard University.	05/30/2025 - 05/31/2025	The complexity of researching emerging threats is compounded by delayed reporting, as adversary tactics continuously evolve and adapt. Rapid shifts in threat behavior, including changes in attack methodologies and deceptive techniques, create challenges in maintaining up-to-date intelligence, making real-time analysis and proactive defense	https://www.weforum.org/stories/2025/05/cybersecurity-cyber-risk-national-policy/

				strategies essential for accurate risk assessment.	
‘FCC launches national security unit to counter state-linked threats to US telecoms’ By: David Jones, Reporter for ‘Cybersecurity Dive’	Media Source	Google as a research tool. Cybersecurity Dive is an online Cyber industry publishing.	05/30/2025 - 05/31/2025	Given the complexity of threats facing national security and critical infrastructure, anticipating the timing and scope of federal decision-making presents a significant challenge. The evolving nature of cyber risks, geopolitical tensions, and technological advancements adds layers of uncertainty, making it difficult to predict which policies will be enacted and when they will yield substantial impact on national resilience and defense strategies.	
‘How Web Scraping Helps	Media Source	Google as a research tool. This article	05/30/2025 - 05/31/2025	Scraped data may be inconsistent or	

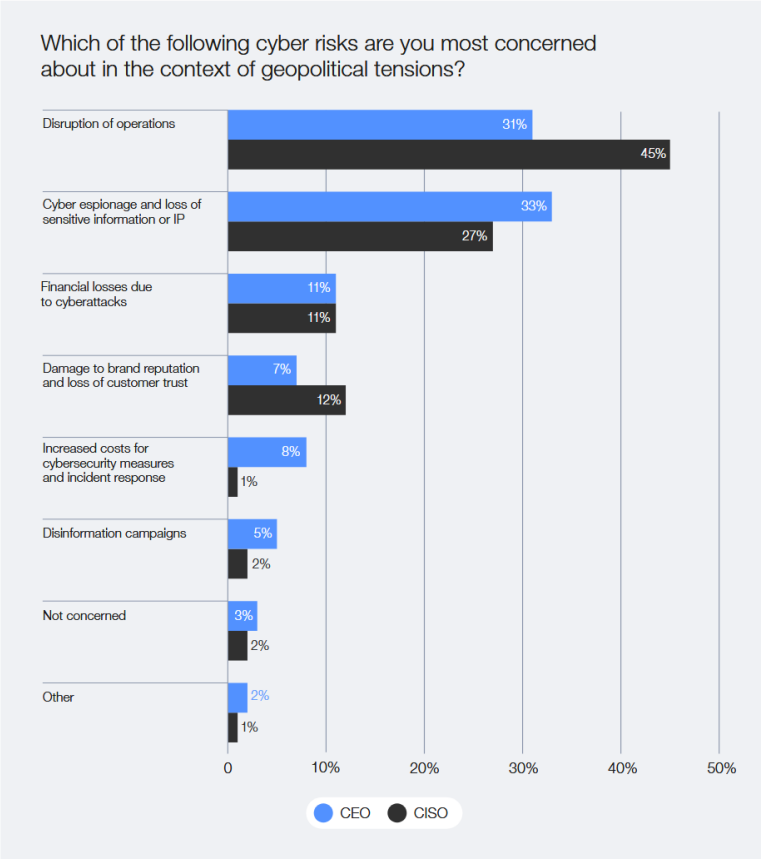
Protect Against Cyber Crimes' By: Oleg Kulyk		presents how a technique used for data extraction can bolster cyber defenses.		manipulated by adversaries. Additionally, scraping can violate privacy laws when performed without permission.	
'Leveraging Open-Source Intelligence (OSINT) Against the Cyber Kill Chain' By: Rohitha Chowdary	Media Source	Google as a research tool. This article presents how mapping OSINT against the Cybersecurity Kill Chain framework can trace the steps of malicious actors and enhance organizations cyber defense efforts against their attack.	05/31/2025 – 06/01/2025	Cybersecurity frameworks provide a strong foundation for organizations to defend against cyber threats, and integrating Open-Source Intelligence (OSINT) can significantly enhance their security posture. However, these frameworks must remain flexible and adaptive, continuously evolving to incorporate real-time OSINT insights. As the threat landscape shifts and malicious actors refine their attack methods, organizations must	

				ensure their frameworks are responsive, leveraging OSINT to anticipate emerging threats and proactively strengthen their defenses.	

The media sources used from federal press releases highlights the growing concerns of malicious state and non-state actors threatening government agencies and private organizations at a global level. The World Economic Forum's Global Cybersecurity Outlook Survey shows that nearly 60% of organizations report that geopolitical tensions have directly influenced their cybersecurity strategy (Heiding 2025). The same survey revealed that 72% of its respondents reported an increase in organizational cyber risks, with ransomware remaining a top concern. In addition, nearly half of global organizations now cite the malicious use of generative AI as their top cybersecurity concern (Heiding 2025). Geopolitical tensions have led to a surge in cyberattacks by state-sponsored adversary groups from China, Russia, and North Korea, targeting both private-sector entities and federal agencies through cyber espionage. Recent survey reports highlight the increasing use of ransomware and adversarial AI technologies to compromise critical infrastructure, steal sensitive data, and exploit intellectual property. In response, organizational leaders and key stakeholders must

prioritize strengthening cyber defense strategies by investing in robust infrastructure, implementing advanced security measures, and promoting comprehensive awareness training to mitigate evolving threats.

The effects of geopolitical tensions on organizations' cybersecurity strategies



Reference: [World Economic Forum Global Cybersecurity Outlook 2025.]

The Federal Communications Commission is launching its own national security unit in response to a series of attacks to U.S. telecom firms. Sophisticated hacks into U.S. telecom firms, which have been attributed to a China-linked threat group called ‘Salt Typhoon’, were seen as part of a larger espionage campaign against the U.S., where the state-linked hackers were able to gain access to calls and other sensitive data as well as intercept the communications of U.S. officials involved in sensitive political and diplomatic work (Jones 2025). Despite being recognized as one of the more mature and cyber-resilient infrastructures, a Chinese hacking group successfully penetrated its firewalls. This incident highlights the urgent need to reassess and fortify cybersecurity defenses against evolving threats. Establishing a dedicated cybersecurity council with a strong commitment to strategic protections for wired, wireless, and satellite networks is essential in safeguarding critical communications infrastructure.

The Center for Strategic & International Studies (CSIS) has documented a timeline of significant cyber incidents dating back to 2006. Over the past four years, my research has revealed that many of these incidents involve state-sponsored groups from adversarial nations, primarily China and Russia. Their cyber activities often align with espionage efforts, including the theft of sensitive data, disinformation campaigns, surveillance operations, and attempts to interfere in elections. These findings highlight the persistent and evolving nature of cyber threats posed by nation-state actors. Utilizing a well-curated list of cybersecurity sources for OSINT strengthens national security strategies in cyberspace by enabling proactive threat detection, intelligence gathering, and strategic decision-making. This intelligence supports incident response efforts, enhances cybersecurity policies, and fortifies critical

infrastructure protection against evolving threats. Additionally, OSINT aids in counterintelligence, allowing national security teams to anticipate adversarial tactics and disinformation campaigns. Significant Cyber Incidents

The rising threat landscape in cyberspace, driven by geopolitical tensions and the increasing sophistication of state-sponsored adversaries, underscores the critical need for enhanced cyber resilience and national security strategies. OSINT plays a vital role in this effort, providing actionable intelligence that enables organizations to detect, analyze, and respond to evolving cyber threats. By leveraging open-source intelligence, security professionals can gain insights into adversarial tactics, identify vulnerabilities, and proactively mitigate risks. As demonstrated by recent attacks on critical infrastructure including the U.S. telecom sector, the importance of continuous intelligence gathering, collaboration, and strategic cybersecurity investments cannot be overstated. Federal agencies such as the Cybersecurity & Infrastructure Security Agency (CISA) a component to the department of Homeland Security provides guidance for cybersecurity best practices for individuals and organizations to manage risks. Cybersecurity & Infrastructure Security Agency.

Web scraping, when integrated with OSINT and cybersecurity, enhances national security by systematically collecting and analyzing publicly available data to identify emerging cyber threats, monitor adversary activities, and safeguard critical infrastructure.

By extracting intelligence from forums, social media, and dark web marketplaces, security agencies can gain real-time insights into cybercriminal operations, state-sponsored attacks, and vulnerabilities that could be exploited. This process involves the use of automated scripts or bots that navigate through web pages to collect information. In the context of cybersecurity, web scraping plays a significant role in identifying and mitigating potential threats by gathering intelligence on cybercriminal activities and vulnerabilities (Kulyk 2024). This proactive approach allows organizations to anticipate cyber threats, detect disinformation campaigns, and track breaches before they escalate. Moreover, web scraping helps security analysts monitor the use of adversarial AI in cyber warfare, ensuring that government institutions and private organizations remain resilient against evolving threats.

Despite its benefits, web scraping for cybersecurity and OSINT presents several challenges. Legal and ethical constraints can limit the collection of certain online data, requiring compliance with privacy regulations and ethical guidelines. The sheer volume of scraped information introduces difficulties in filtering false positives, demanding sophisticated verification methods to ensure intelligence accuracy. Additionally, cyber adversaries often deploy countermeasures such as encryption, anonymization, and misinformation tactics to evade OSINT tracking, making detection efforts more complex. Specialized tools such as web crawlers, automated data parsers, and sentiment analysis software help security teams efficiently process and categorize scraped data.

MITRE Att&ck Framework

The MITRE ATT&CK framework is a powerful tool for understanding and mitigating cyber threats, particularly in national security contexts. It provides a comprehensive, structured repository of adversary tactics, techniques, and procedures (TTPs), helping security teams anticipate, detect, and respond to cyber threats effectively. Combining MITRE ATT&CK with OSINT can be powerful in national security strategies, it is imperative to navigate challenges carefully to ensure accurate and actionable intelligence.

MITRE ATT&CK Benefits:

- It can be used to perform threat intelligence and profiling for analysts to understand adversary behavior. Understanding their motives to Cyber espionage attacks allow for proactive defense.
- The Att&ck framework is globally recognized so organizations across military, intelligence, and government sectors can share threat intelligence more efficiently.
- With the use of the intelligence, 'Red Team' simulations can be conducted to improve cyber defenses on infrastructure.

MITRE ATT&CK Challenges:

- The vast amount of available information makes filtering out false or misleading intelligence difficult.
- Legal and ethics boundaries to which government agencies must balance national security needs with privacy concerns and legal restrictions on data collection.
- Aligning raw OSINT findings with ATT&CK's structured framework, as cybercriminals constantly evolve their methods. Continuous OSINT feeds will be necessary for the framework to adapt.

NIST Cybersecurity Framework v2.0

With its emphasis on governance, risk management, and threat detection, the framework helps national security teams integrate OSINT into proactive cybersecurity strategies. By leveraging open-source intelligence, organizations can align their threat analysis with NIST's core functions—**Identify, Protect, Detect, Respond, and Recover**, enabling more effective monitoring of cyber adversaries, data breaches, and disinformation campaigns.

Adversaries continuously evolve their tactics, employing encryption, obfuscation, and deceptive narratives to evade OSINT tracking, complicating attribution efforts. Legal and ethical concerns surrounding data collection can also pose constraints, requiring

compliance with privacy regulations and responsible intelligence gathering practices. Furthermore, aligning raw OSINT findings with the structured risk management framework demands advanced analytics and AI-driven processing to maintain efficiency. Overcoming these challenges requires strong collaboration between government agencies, cybersecurity professionals, and private-sector stakeholders to ensure that OSINT remains a valuable tool in national security and cyber defense.

Cyber Kill Chain

The 7 Stages of a Cyber Attack

1 Reconnaissance
Attackers gather info on the target to find vulnerabilities.

2 Weaponization
Malware or exploits are created to target those weaknesses.

3 Delivery
The malicious payload is sent via phishing, web, or physical media.

4 Exploitation
The payload activates, exploiting a flaw to gain access.

5 Installation
Malware is installed to maintain access.

6 Command & Control (C2)
The system connects to attacker servers for remote control.

7 Actions on Objectives
Attackers achieve their goals like data theft or disruption.

The Cyber Kill Chain framework 2.0 enhances OSINT capabilities in cybersecurity and national security by providing a structured methodology for identifying, analyzing, and mitigating cyber threats. The framework, originally developed by Lockheed Martin, outlines the various stages of a cyberattack, from reconnaissance to data exfiltration, allowing security teams to use OSINT to track adversarial activities before, during, and after an attack. By leveraging open-source intelligence, analysts can detect early indicators of compromise, assess adversary tactics, and correlate findings with Cyber Kill Chain stages to predict potential attack vectors. This integration enables proactive threat intelligence, strengthening national security efforts against cyber espionage, ransomware, and AI-driven attacks.

The Cyber kill chain has similar limitations comparable to the NIST and the MITRE Att&ck frameworks involving the risk of the validation of the data and privacy breach laws. Another limitation is the dynamic nature of cyberattacks, where threat actors may bypass traditional kill chain stages by using advanced techniques like zero-day exploits and AI-powered attacks, requiring security teams to continuously refine OSINT methodologies. Deep threat intelligence platforms, advanced analytics technologies, and cross-functional efforts by Cybersecurity professionals and government agencies will be critical to ensure resilience and national security posture.

SOURCES

Jones, David (2025, March 13): '*FCC launches national security unit to counter state-linked threats to US telecoms*', https://www.cybersecuritydive.com/news/fcc-national-security-council/742440/

Heiding, Frederik (2025, May 13): '*72% of cyber leaders say risks are rising. Here's how states and businesses are responding*',

https://www.weforum.org/stories/2025/05/cybersecurity-cyber-risk-national-policy/

World Economic Forum; Accenture (2025, January): '*Global Cybersecurity Outlook 2025*'.
https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

Center For Strategic & International Studies 'CISA' (2025, April): '*Significant Cyber Incidents*',
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Cybersecurity & Infrastructure Security Agency; Topics (2025, May): '*Cybersecurity Best Practices*',
https://www.cisa.gov/topics/cybersecurity-best-practices

Kulyk, Oleg (December 02, 2024): '*How Web Scraping Helps Protect Against Cyber Crimes*', https://scrapingant.com/blog/web-scraping-against-cyber-crimes

National Institute Standards Technology (2025, May): 'Cybersecurity Framework 2.0', https://www.nist.gov/cyberframework

MITRE ATT&CK (2025, May): '*ATT&CK Matrix for Enterprise*', https://attack.mitre.org/#

Lockheed Martin (2025, May): '*The Cyber Kill Chain*', https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Chowdhary, Rohitha (2023, July 07): '*Leveraging Open-Source Intelligence (OSINT) Against the Cyber Kill Chain*',
https://www.optiv.com/insights/discover/blog/leveraging-open-source-intelligence-osint-against-cyber-kill-chain