THE PANKAJ KUMAR JHA
CENTRE FOR SECURITY STUDIES | ISSUE BRIEF

JANUARY 2025

STATE OF GLOBAL WARFARE: TECHNOLOGICAL DEVELOPMNETS AND DANGERS

Jay Talewar

Edited by: Sai Vira Gupta

About the Author

Jay Talewar is a postgraduate student at the Jindal School of International Affairs and is a Research Intern at the Pankaj Kumar Jha Centre for Security Studies, JSIA.

About the Pankaj Kumar Jha Centre for Security Studies

The Pankaj Kumar Jha Centre for Security Studies (PKJCSS) was established in 2020 as the Jindal School of International Affairs' first student-run research centre under the aegis of Prof. Dr. Pankaj K. Jha. Researchers at PKJCSS explore both regional and thematic topics in the broader field of international security studies to write issue briefs, policy briefs, defence white papers, and dialogue session reports on contemporary issues. The concept of international security has been expanded to reflect not merely the study of state security, but also include topics like ethnic, sectarian, and religious conflict; civil wars and state failure; cyber and space warfare; resource-related security issues; the proliferation of weapons of mass destruction; defence economics and the role of ethics or morality in the formulation of security policies. The complexity of these matters is what the Pankaj Kumar Jha Centre for Security Studies attempts to unfold. Please refer to www.cssjsia.com for further details, and follow the Centre's social media platforms for critical news and research updates:


www.linkedin.com/company/jindal-centre-for-security-studies/


www.instagram.com/css_jsia/


https://twitter.com/Css_Jsia

Get in touch with us through email: css@jgu.edu.in

Important disclaimer

IB250104

Introduction

The ever-changing scenario of cybersecurity is the reason for the unprecedented growth of sophisticated cyber threats in countries. Advanced technologies, including artificial intelligence (A.I.), expert systems, Web 4.0, and natural language processing (NLP), are progressing rapidly, requiring stringent security measures to prevent exploitation by malicious actors. Cybersecurity refers to protecting networks and data against digital attacks, which have become a matter of concern.[1] This category involves unauthorised access and security breaches. Superpowers and developed nations are within the list that comprises their counterparts in the United States and other world powers. China, Russia, Israel, India, France, Germany, the United Kingdom, and some Arab nations were some of the intruders themselves, even using malicious applications. Recent improvements have required greater security for such cyberattacks.

That means security is comparable to having a bulletproof vest. More focus is on anomaly detection and faults within a system that can leak. Firewalls, intrusion detection, and real-time monitoring for anomalies can include any other tool. Encryption makes confidential data secure. If set right, A.I. may be able to pick out patterns to ensure that the cyberattacks are on before they have begun.[2] These enable systems to operate continuously without vulnerabilities to new threats, opening to techniques such as sandboxing, multi-factor authentication, and updates. This also facilitates a system that continues operating with much-reduced vulnerability to new emerging threats. Its interaction depicts how innovation with cybersecurity measures not only addresses existing risks but also helps lay the foundations for a bright, digital, secure future ahead. Even hacking incidents are raising new high-level threats that cause unauthorised access, manipulation, or interference. The interrelationship of economic growth with security and cybersecurity has really underlined the necessity for highlighting national security strategies effectively to face digital threats. Cyber threat management encompasses a set of activities, including detailed

[1] Brooks, C. (2023, March 14). Cybersecurity Trends & Statistics for 2023; What you need to know. *Forbes*. https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/

[2] U.S. Department of the Treasury. (2024). *Managing Artificial Intelligence-Specific cybersecurity risks in the financial services sector*. https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf

vulnerability assessments, in-depth threat intelligence studies, risk mitigation plans, and other activities that aim effectively to counter cyberattacks.

Technological advancement, however, provides the necessary tools to track the perpetrators and monitor the risks, such as when the Stuxnet Virus targeting Iran's nuclear activities was discovered, and therefore shows the strength of cyber intelligence.[3] These solutions actively address challenges, including recognising Russian propaganda campaigns on social media, but human oversight is still inevitable to counter such adversaries. Technology is bringing about new capabilities, including the neutralisation of an attacker and new security architecture improvements.[4] These new measures can be added with sustained security awareness to significantly reduce the tremendous risks posed by cyberattacks. Such is the intensity of these problems, effectively put into words by the renowned Bertrand Russell's declaration: "*Science can teach us, and I think our hearts can teach us, no longer to look around for imaginary supporters, no longer to invent allies in the sky, but rather to look to our own efforts here below to make the world a fit place to live.*" By considering how all these factors are related through the advancement of technology, human responsibility, and anticipatory security practice, governments are even better placed to navigate these complicated difficulties of the digital age.

What do we mean by a Cyberattack?

Cyberattack is the use of tech to threaten, defuse, or ransom someone by one or an organisation, often damaging its communication, capacity, and security in the process. Examples of such attacks include viruses like ransomware, navigation hacks, and data leak threats. Such an assault is usually done anonymously and is intended to inflict financial damages or harm the other party without open confrontation.[5] Such an attack is conducted secretly to incite the other side economically or

[3] The Editors of Encyclopaedia Britannica. (2024, November 8). *Stuxnet | Definition, Origin, Attack, & Facts*. Encyclopaedia Britannica. https://www.britannica.com/technology/Stuxnet?utm_
[4] U.S. Cyber Command. (n.d.). *Russian disinformation campaign "DoppelGänger" unmasked: a web of deception*. https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception/
[5] *Cybersecurity in the AI era: How the threat landscape evolved in 2023*. (2023, December 11). /. https://www.kaspersky.com/about/press-releases/cybersecurity-in-the-ai-era-how-the-threat-landscape-evolved-in-2023

injure them psychologically without even a direct collision. Still, the occurrence of cyberwarfare by the cyberattack on the 2024 Baltimore Bridge and its happening shows how cyber can have concrete effects in the real world. It is reported that during this type of attack, the attackers seized the operation systems on the bridge, which resulted in serious technological problems there. From this collapse, vehicular accidents and deaths were realised, leaving the flow of traffic in a paralysed state for quite some time.[6] Such events show vulnerability in critical infrastructure and the high stakes for public safety, bringing out the urgency for comprehensive cyberdefence strategies. It goes into an even broader tale: of how the cyber domain connects with actual security, where cyberattacks, according to the given paper and literature, go far beyond just some sort of virtual side effect.

These developments have great significance in pointing out the essential necessity for countries to work on their cyber readiness and amend their military doctrines in the face of the changing nature of cyber conflict. The growing connectivity, scope, and sophistication of cyberattacks present a quite wide range of challenges involving attribution to escalation control and combining cyber operations into the traditional planning of the military. For example, there is a computer worm called Stuxnet that attacked Iranian nuclear installations in 2010-the landmark indication of the possible ability to bring down critical infrastructure without overt traditional military actions. A wake-up call has been given to international systems, stating that even firmly secured facilities are susceptible to nation-state cyber activities. Similarly, cyberattacks on Estonia in 2007 were the first significant use of coordinated Distributed Denial of Service (DDoS) attacks to disable a country's digital infrastructure, targeting government websites, financial institutions, and media organisations. The events brought into focus the possibility of digital tools being used as weapons in pursuit of political and strategic objectives, and therefore, there is a need for robust cybersecurity measures and international standards to counter such threats.[7]

[6] Insurance, K. (2024, March 27). *Was cyber-attack behind Francis Scott Key Bridge collapse?* https://www.koop.ai/blog/cyber-insurance-on-the-edge-was-the-baltimore-bridge-incident-a-cyber-attack
[7] *Connect the Dots on State-Sponsored Cyber Incidents - Estonian denial of service incident*. (n.d.). Council on Foreign Relations. https://www.cfr.org/cyber-operations/estonian-denial-service-incident?utm_source=chatgpt.com

Since the annexation of Crimea in 2014, continuous streams of cyberattacks attributed to Russian agents have been faced in Ukraine.[8] These cyber breaches resulted in highly elevated levels of disruption as well as loss by affecting major domains, namely financial institutions, energy infrastructures, and governmental systems. For instance, 2017 NotPetya primarily targeted business houses in Ukraine before causing a global influence.[9] The malware was so aggressive that it shut down the operations and brought more than $300 million in losses to companies like Maersk. NotPetya showed the cyberattack capability to cross geographical lines, disrupt worldwide supply chains, and further plunge an already volatile region into more profound economic and political instability. An analysis of the ripple effects from this kind of attack shows that cyber incidents should not be seen as isolated events, but rather as intentional processes meant to weaken opponents while further eroding public confidence in critical systems.

Cyberattacks result in cascading consequences such as social unrest, economic downfall, and even unemployment. The infrastructural disruption is usually worse than the actual living conditions within the affected nations. Cybercrime may knock out a country's major sectors, such as transport, with mass production of falsely malfunctioning electronically integrated products or disabling navigation systems, which will trigger delays and accidents. Specially trained government-sponsored programs can create intelligence misinformation that jeopardises the security of a nation to global instability.[10] This is because the states, such as Russia, China, and Iran, have themselves involved in cyber espionage and information suppression in their broader geopolitical strategies. Such state-sponsored cyber operations further destabilise the global security domain, and thus the need for international cooperation and legal frameworks is further highlighted in addressing such emerging challenges.

NLP in the context of Cybersecurity

[8] Russia's war on Ukraine: Timeline of cyber-attacks. (2022). In *EPRS | European Parliamentary Research Service* (Report PE 733.549). https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf
[9] Steinberg, S., Stepan, A., Neary, K., & Picker Center Digital Education Group. (2021). NotPetya: A Columbia University case study. *SIPA*. https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf
[10] Delerue, F. (2016). *State-sponsored cyber operations and international law*. https://doi.org/10.2870/55936

NLP is considerably on the rise in cybersecurity as organisations fight back against advanced threats that involve linguistics. NLP helps to analyse unstructured data like phishing attacks, malicious communications, and other social media postings to understand vulnerabilities. Techniques like sentiment analysis and named entity recognition through applications help NLP systems gain insight into why malicious actors are malicious and, hence, have become a vital component in modern security infrastructure. For instance, NLP tools can be used to scan email communications and public posts for possible vulnerabilities and emerging attack vectors, thus keeping organisations aware and better prepared.[11]

NLP encompasses a whole host of methods that give the computer the ability to interpret human language. Essentially, the basic techniques include tokenisation, the process of breaking down text into smaller units, known as tokens, and tagging, where every word in a sentence is assigned a specific grammatical role. When combined with deep learning, these techniques have broadened the scope of NLP applications far beyond cybersecurity. The current models, BERT and GPT-3, enable excellent pattern recognition, which enables NLP applications to range from automating customer services to threat identification.[12] This has enabled cyber experts to successfully repel such powerful attacks. Web 4.0 is commonly referred to as the "Intelligent Web," encompassing all the characteristics of technological advancement. This paradigm involves integrating higher-order technologies, such as AI and NLP, in everyday experience to create this hyper-personalised, efficient nature of cyberspace.[13] However, it also raises the newest vulnerabilities to be exploited by cyber warfare. NLP technologies will be able to identify hostile intentions, predict future threats, and take steps to automate responses once an incident has occurred. Conversely, malicious people are becoming increasingly likely to exploit AI-based resources to do reconnaissance and plan their attacks.[14] For this reason, these resources further enable phishing and social engineering

[11] *NLP and Cybersecurity: Detecting Threats in Human Language – Veritas NLP*. (n.d.). https://veritasnlp.com/nlp-and-cybersecurity-detecting-threats-in-human-language/
[12] Ceresnak, R., PhD. (2024, November 24). The rise of AI Chatbots: How GPT-3 and BERT are redefining conversational experiences. *Medium*. https://medium.com/codex/the-rise-of-ai-chatbots-how-gpt-3-and-bert-are-redefining-conversational-experiences-4f3f19bb67e6
[13] Espinosa, C., & Espinosa, C. (2024, February 14). Transforming Cybersecurity with AI and NLP - Blue Goat Cyber. *Blue Goat Cyber*. https://bluegoatcyber.com/blog/transforming-cybersecurity-with-ai-and-nlp/?utm_
[14] Concannon, M. (2024, July 16). AI in social Engineering: the next generation of cyber threats. *Ntiva*. https://www.ntiva.com/blog/ai-social-engineering-attacks?utm_

because they enable more complex and targeted deceptions, which are most likely to bypass even current defences.

This interconnectivity of digital communications makes the cybersecurity landscape even more complicated, as in the case of Russian interference in the 2016 United States elections.[15] This interference relied heavily on social media platforms for the diffusion of disinformation and for the manipulation of public opinion. The expansion of communication networks, although it promotes connectivity, reduces barriers to the execution of such operations. An analysis of these events shows that NLP plays a critical role in the detection and mitigation of linguistic-based threats, emphasising its value in modern cybersecurity frameworks.

Conclusion

The advent of cyber warfare brings a new dimension to global security, offering both opportunities and huge threats. Significant incidents such as the Stuxnet virus, the SolarWinds breach, and ransomware attacks on vital infrastructure illustrate how cyberattacks can easily transcend national boundaries and challenge global stability.[16] The Stuxnet case demonstrated the capability of cyber tools to covertly damage critical infrastructure by explicitly targeting Iran's nuclear program, all without resorting to conventional military conflict. In its international supply chain, the incident further showed vulnerabilities wherein adversaries penetrated a lot of systems, resulting in the exposure of sensitive information to further drain trust within necessary digital infrastructure. All this drives home the strategic significance of cyber warfare towards the achievement of political, economic, and military objectives. The current Russia-Ukraine war further puts into perspective how serious contemporary cyber operations can be.

Cyberattacks against Ukraine have continued unabated since the annexation of Crimea by Russia in 2014, including, famously, the ransomware attack by NotPetya in 2017, which began first against institutions in Ukraine before turning into a global attack against industry, costing billions.

[15] U.S. Department of Justice, & Mueller, R. S., III. (2019). Report on the investigation into Russian interference in the 2016 presidential election. In *Volume II*. https://www.justice.gov/storage/report_volume2.pdf
[16] *The SolarWinds Cyber-Attack: What you need to know*. (2021, November 9). CIS. https://www.cisecurity.org/solarwinds

These kinds of operations create chaos in systems, cause collapse in infrastructure, and make socio-economic crises worse.[17] Such evidence is illustrative of how cyber war alters the contours of a conflict wherein destabilisation and disruption supersede traditional warfare action. Cyberattacks are a critical threat not only to national security but also to world stability, threatening essential services, trade relations, and cooperative actions in environmental protection.

The interdependent features of global networks heighten these risks and require proactive measures by governments, industries, and international organisations. The modern technologies of artificial intelligence, machine learning, and advanced encryption offer potential cures but also create complex vulnerabilities.[18] The balance between taking advantage of these technological developments and managing their risks will determine the future of cybersecurity. These activities will need mutual responsibility from the stakeholders. Countries should spend their budget on technological advancements, defence systems, and international cooperation to establish an efficient cybersecurity infrastructure[19]. These activities will prepare communities with the capacity to react appropriately towards the growing implications of cyber warfare. Vigilance, innovation, and collective effort will be needed in the near future to protect critical systems in an increasingly dynamic cyberspace.

[17] *Global financial stability is at risk due to cyber threats, the IMF warns. Here's what needs to happen*. (2024, September 10). World Economic Forum. https://www.weforum.org/stories/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/?utm_

[18] Rota, D. (2018, November 8). *A Quantum Leap in International Law on Cyberwarfare: An Analysis of International Cooperation with Quantum Computing on the Horizon | Harvard National Security Journal*. https://harvardnsj.org/2018/11/08/a-quantum-leap-in-international-law-on-cyberwarfare-an-analysis-on-the-need-for-international-cooperation-with-quantum-computing-on-the-horizon/

[19] *Strategies to Deter and Respond to Cyber Operations in Conflict - Digital Front Lines*. (2023, August 2). https://digitalfrontlines.io/2023/08/02/strategies-to-deter-and-respond-to-cyber-operations/

Bibliography

1. Brooks, C. (2023, March 14). Cybersecurity Trends & Statistics for 2023; What you need to know. *Forbes*. https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/
2. Concannon, M. (2024, July 16). AI in social Engineering: the next generation of cyber threats. *Ntiva*. https://www.ntiva.com/blog/ai-social-engineering-attacks?utm_
3. *Connect the Dots on State-Sponsored Cyber Incidents - Estonian denial of service incident*. (n.d.). Council on Foreign Relations. https://www.cfr.org/cyber-operations/estonian-denial-service-incident?utm_
4. *Cybersecurity in the AI era: How the threat landscape evolved in 2023*. (2023, December 11). /. https://www.kaspersky.com/about/press-releases/cybersecurity-in-the-ai-era-how-the-threat-landscape-evolved-in-2023
5. Delerue, F. (2016). *State-sponsored cyber operations and international law*. https://doi.org/10.2870/55936
6. Espinosa, C., & Espinosa, C. (2024, February 14). Transforming Cybersecurity with AI and NLP - Blue Goat Cyber. *Blue Goat Cyber*. https://bluegoatcyber.com/blog/transforming-cybersecurity-with-ai-and-nlp/?utm_
7. *Global financial stability is at risk due to cyber threats, the IMF warns. Here's what needs to happen*. (2024, September 10). World Economic Forum. https://www.weforum.org/stories/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/?utm_
8. Insurance, K. (2024, March 27). *Was cyber attack behind Francis Scott Key Bridge collapse?* https://www.koop.ai/blog/cyber-insurance-on-the-edge-was-the-baltimore-bridge-incident-a-cyber-attack
9. *NLP and Cybersecurity: Detecting Threats in Human Language – Veritas NLP*. (n.d.). https://veritasnlp.com/nlp-and-cybersecurity-detecting-threats-in-human-language/
10. Rota, D. (2018, November 8). *A Quantum Leap in International Law on Cyberwarfare: An Analysis of International Cooperation with Quantum Computing on the Horizon | Harvard National Security Journal*. https://harvardnsj.org/2018/11/08/a-quantum-leap-in-

international-law-on-cyberwarfare-an-analysis-on-the-need-for-international-cooperation-with-quantum-computing-on-the-horizon/

11. Russia's war on Ukraine: Timeline of cyber-attacks. (2022). In *EPRS | European Parliamentary Research Service* (Report PE 733.549). https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf
12. Steinberg, S., Stepan, A., Neary, K., & Picker Center Digital Education Group. (2021). NotPetya: A Columbia University case study. *SIPA*. https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf
13. *Strategies to Deter and Respond to Cyber Operations in Conflict - Digital Front Lines*. (2023, August 2). https://digitalfrontlines.io/2023/08/02/strategies-to-deter-and-respond-to-cyber-operations/
14. *Ceresnak, R., PhD. (2024, November 24). The rise of AI Chatbots: How GPT-3 and BERT are redefining conversational experiences. Medium.* https://medium.com/codex/the-rise-of-ai-chatbots-how-gpt-3-and-bert-are-redefining-conversational-experiences-4f3f19bb67e6
15. The Editors of Encyclopaedia Britannica. (2024, November 8). *Stuxnet | Definition, Origin, Attack, & Facts*. Encyclopedia Britannica. https://www.britannica.com/technology/Stuxnet?utm_
16. *The SolarWinds Cyber-Attack: What you need to know*. (2021, November 9). CIS. https://www.cisecurity.org/solarwinds
17. U.S. Cyber Command. (n.d.). *Russian disinformation campaign "DoppelGänger" unmasked: a web of deception*. https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception/
18. U.S. Department of Justice, & Mueller, R. S., III. (2019). Report on the investigation into Russian interference in the 2016 presidential election. In *Volume II*. https://www.justice.gov/storage/report_volume2.pdf
19. U.S. Department of the Treasury. (2024). *Managing Artificial Intelligence-Specific cybersecurity risks in the financial services sector*.

https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf