The Information Domain of 2030: Data Exploitation as Weapons of the Future

Khair, Rayhan Imamul

** The Cyber Warfare of 2030: Data Exploitation as Weapons of the Future, illustrated by AI.*

As we near a new decade, the scale of the evolving digital landscape is nearly impossible to comprehend. The Information Domain of 2030 isn't simply a continuation of today's trends; it's a complex environment in which data becomes a decisive front in every battle. As technology becomes more integrated into the fabric of daily life, data protection and exploitation are emerging as new frontiers in global strategic competition. This essay aims to uncover the potential trajectories of cyber influence and the darker undercurrents that may alter international relations and security dynamics. To begin with, I will comprehensively analyze the information domain as a critical component of future warfare, then examine the implications of technological advancements and forecast the comprehensive approach and strategy to face the challenge.

Introduction: how the information domain plays in conflicts

Historically, conflict produced tangible imagery: battlefields, trenches, and artillery. Khorram-Manesh and Burke define conventional warfare as conflicts between regulated militaries or states employing traditional military tactics and weaponry.[1] However, I suggest that the information realm functions beyond the confines of conventional warfare paradigms. Razma emphasizes this perspective, noting that unconventional warfare is distinguished from its conventional counterpart through unique strategies and tactics.[2] The United States (US) is advancing this concept by embracing the Revolution in Military Affairs (RMA). Ganske explains RMA as a radical change in military strategy, doctrine, and technology-driven by the advent of advanced information technology and precision weaponry.[3] This shift, which Niva argues began before 2001, saw the U.S. military integrating networked information technology as a core component of its operations.[4] The RMA's impact was evident in the U.S. military's experiences in the 1991 Gulf War and the aerial war in Kosovo. In these conflicts, using satellites, “smart” weapons, and advanced communications technology significantly enhanced the US's capabilities against traditional military operations. In this new era, the frontlines are digital firewalls, and the soldiers are lines of code. The stakes in this warfare domain are immensely high, reflecting the transformative effects of RMA on modern military strategies.

[1] Amir Khorram-Manesh and Frederick M. Burkle, “Civilian Population Victimization: A Systematic Review Comparing Humanitarian and Health Outcomes in Conventional and Hybrid Warfare,” *Disaster Medicine and Public Health Preparedness* 17 (January 2023): e192, https://doi.org/10.1017/dmp.2022.96.
[2] Gintautas Razma, “A Modern Warfare Paradigm: Reconsideration of Combat Power Concept,” *Journal of Security and Sustainability Issues* 8, no. 3 (2019): 435–52, https://doi.org/10.9770/jssi.2019.8.3(12).
[3] “Why RMAs Still Matter,” accessed December 13, 2023, https://thestrategybridge.org/the-bridge/2016/1/3/why-rmas-still-matter?format=amp.
[4] Steve Niva, “Disappearing Violence: JSOC and the Pentagon’s New Cartography of Networked Warfare,” *Security Dialogue* 44, no. 3 (2013): 185–89, https://doi.org/10.1177/0967010613485869.

Unlike a traditional battlefield with localized impacts, a strike within the information domain could have global repercussions, such as destabilizing financial markets, swaying political decisions, or exposing national defense strategies. Guadagno and Guttieri mention that misinformation and disinformation can influence the public cognitively into beliefs about a specific topic or indirectly create delusion or confusion despite evidence to the contrary.[5] Data breaches and information exploitation will be used strategically to manipulate public opinion, undermine trust in institutions, and disrupt societal norms. Exploiting data will benefit adversaries by gaining an "information advantage."[6] Data exploitation will become a weapon when used to influence "cognitive bias" and create confusion, thereby enabling the adversary to achieve goals that traditionally have been pursued through more overt forms of espionage or warfare.[7] The key to utilizing this weapon lies in understanding the psychological and social dynamics of the targeted population and leveraging technology to manipulate these dynamics in one's favor.

The compromise of personal data involving millions of federal employees in the United States (US) has highlighted the susceptibility of domestic databases to intrusion by foreign intelligence agencies. The 2015 breach at the US Office of Personnel Management aptly illustrated the strategic ramifications of data intrusions by compromising personal information belonging to

---

[5] Rosanna E. Guadagno et al., "Fake News and Information Warfare: An Examination of the Political and Psychological Processes From the Digital Sphere to the Real World," chapter, https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-7998-7291-7.ch013 (IGI Global, January 1, 1AD), 25–28, fake-news-and-information-warfare, https://www.igi-global.com/gateway/chapter/www.igi-global.com/gateway/chapter/269096.

[6] Information Adventages is defined as Informational power is the ability to use information to support achievement of objectives and gain an information advantage. The essence of informational power is the ability to exert one's will through the projection, exploitation, denial, and preservation of information in pursuit of objectives. *JP 3-04 Information in Joint Operations*, 4th ed., 2022, II–2.

[7] Haselton and Nettle emphasized the "cognitive bias" that human cognition is frequently distorted, including estimates of the impact time of approaching objects and projections of future social outcomes Martie G. Haselton, Daniel Nettle, and Paul W. Andrews, "The Evolution of Cognitive Bias," in *The Handbook of Evolutionary Psychology* (John Wiley & Sons, Ltd, 2015), 64, https://doi.org/10.1002/9780470939376.ch25.

more than 22 million individuals, including government contractors and employees.[8] The compromised information may have been utilized to ascertain the identities of victims, monitor their whereabouts, deduce their motivations, monitor their international travel, correspondence, and contacts, pinpoint susceptibilities for recruitment purposes, facilitate network intrusion and computer hacking, target for human intelligence gathering, disparage, blackmail, or exact vengeance, or endanger the safety of individuals and the national and international community through the use of challenges to their security.

The effect of exploitation of leaked data can reveal a country's tactics, vulnerabilities, and assets that jeopardize national security-sensitive information used for effective cyberattacks. The attack can affect essential infrastructure, potentially disrupting water supplies, transportation networks, and electricity utilities. Consider how China proxy hackers targeted American infrastructure in 2023, risking the country's security.[9] Historically, espionage operations relied on physical papers and human operators. As technology advances, espionage operations are increasingly conducted digitally, enabling faster and potentially more devastating operations.

Data breach incidents exhibited significant changes between 2018 and 2023, compromising 217 million user accounts by the third quarter of 2023.[10] By 2030, data breaches will advance to encompass information theft, increasing the likelihood of cyber surveillance, cyber-attacks, and espionage. The concerning aspect is that stolen data might be utilized to train neural networks for predictive modeling of behaviors, enabling the manipulation of societies through targeted

[8] "Office of Personnel Management Data Breach (2015)," International cyber law: interactive toolkit, June 4, 2021, https://cyberlaw.ccdcoe.org/wiki/Office_of_Personnel_Management_data_breach_(2015).
[9] "Alaska Dispatch: Chinas Cyber Army Is Invading Critical U.S. Services - ProQuest," accessed January 31, 2024, https://www.proquest.com/docview/2900632176?parentSessionId=hS6OL0K2yAWvijSWJOnplX27m0%2FXuea%2BIerBLfNn0WQ%3D&pq-origsite=primo&accountid=12702&sourcetype=Newspapers.
[10] "Data Breach Statistics: Q3 2023," Surfshark, accessed November 8, 2023, https://surfshark.com/research/study/data-breach-statistics-q3-2023.

propaganda. The current situation highlights the urgent requirement for sophisticated cybersecurity measures to prevent the growing risk of data exploitation and information manipulation in the era of cyber warfare.

The future direction of weaponizing the information domains

Another scholar underlines the future threat of artificial intelligence (AI). Dunn et al. highlight the high danger of data poisoning attacks on machine learning models.[11] These attacks involve injecting harmful data into the training dataset and drastically degrading the model's performance. The breaches may enable adversaries to introduce malware or fabricated data that corrupts the A.I. machine learning process. As a result, the infiltrated system may use this A.I. output to disseminate disinformation.

Through its advancements, deepfake technology will heighten existing risks. Although deepfakes showcase the AI's capabilities, they potentially generate significant dangers. They can spread misinformation and manipulate public opinion by creating highly realistic fake videos, images, and audio.[12] In politics, deepfakes can undermine trust in officials or influence elections through falsified recordings. Furthermore, this deepfake technology can risk privacy violations in personal contexts by generating non-consensual explicit content or harmful impersonations.[13] From a legal perspective, deepfakes present challenges. The current laws may not adequately address AI-generated content, thus making it hard to combat the misuse of deepfake. As this

[11] Corey Dunn, Nour Moustafa, and Benjamin Turnbull, "Robustness Evaluations of Sustainable Machine Learning Models against Data Poisoning Attacks in the Internet of Things," *Sustainability* 12, no. 16 (January 2020): 6434, https://doi.org/10.3390/su12166434.
[12] Britt Kaeli, "How Are Deepfakes Dangerous?" University of Nevada, Reno, March 31, 2023, https://www.unr.edu/nevada-today/news/2023/atp-deepfakes.
[13] Kaeli.

technology becomes more accessible and sophisticated, it creates difficulties distinguishing real from fake content, while it needs effort to complicate fact-checking and verification efforts.

Because of the spread of misinformation, this advanced technology can potentially erode public confidence in the media and institutions. This spread of misleading information can be demonstrated in several ways, from deliberate leaks intended to affect political or economic prospects to disinformation campaigns that utilize facts to deceive populations. Therefore, despite deepfake technology's demonstration of advanced artificial intelligence, the country should consider any urgent discussions on ethics, legal frameworks, and detecting methods to lessen its possibly harmful impacts.

How will the nations answer the challenges in the future?

The future of information warfare will be a complex environment, especially with the advancement of technology and information. Thus, nations need a comprehensive approach that prioritizes cybersecurity and innovative solutions. These strategies include establishing cyber forces, enhancing collaboration and partnership with the international community, private sector engagement and innovation, and media collaboration for public awareness. Those strategies hopefully can optimize the nation's preparation to face dynamic ranges of potential cyber threat scenarios.

Establishing Cyber Force

Establishing a capable cyber force is essential to enhancing a nation's cyber security. The military should pivot the recruitment program and the basic training with a clear path to the outcome of cybersecurity professionals. On the other hand, the government can invest its capital through advanced university courses, specialized training programs, and continuous professional development. Promoting cybersecurity careers via scholarships, internships, and career development is a prominent way to cultivate a resilient cyber force.

Several countries have created specific cyber forces or units within their military or intelligence structures, recognizing the increasing significance of cybersecurity and information warfare in today's world. These forces protect against cyber threats and execute offensive cyber operations. Here are some examples:

a. US: The US Cyber Command (USCYBERCOM) is a mighty force designed to involve "directing, synchronizing, and coordinating cyberspace planning and operations."[14] What the establishment of USCYBERCOM demonstrates is the US understanding of the cyber realm as a central battleground for national security and military projection.

b. China: China possesses cyber capabilities through its Strategic Support Force. This force is primarily focused on space, cyber, and electronic warfare.[15] China's investment in cyber forces is consistent with the country's larger goal of becoming a global leader in information technology and cyber power.

c. Russia: Russia has incorporated cyber activities into its military strategy with various offensive and defensive actors well beyond the military structure.[16] Russia has used its

[14] "CYBER 101 - U.S. Cyber Command Mission," U.S. Cyber Command, accessed November 29, 2023, https://www.cybercom.mil/Media/News/Article/3192016/cyber-101-us-cyber-command-mission/https%3A%2F%2Fwww.cybercom.mil%2FMedia%2FNews%2FArticle%2F3192016%2Fcyber-101-us-cyber-command-mission%2F.
[15] Lyu Jinghua, "What Are China's Cyber Capabilities and Intentions?," Carnegie Endowment for International Peace, accessed November 29, 2023, https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734.
[16] Andrei Soldatov Borogan Irina, "Russian Cyberwarfare: Unpacking the Kremlin's Capabilities," CEPA, September 8, 2022, https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/.

cyber forces to engage in a robust range of cyber actions, illustrating the country's use of cyber warfare as a tool of state policy.

d. United Kingdom (UK): The UK established the National Cyber Force (NCF). NCF became the pioneer in integrating cyber security measures between the UK military service and the government, such as GCHQ, MI6, and the Ministry of Defense. [17]

e. Israel: The Israel Defense Forces Unit 8200, akin to the US National Security Agency, is known for superior cyber capabilities. [18] Such a unit's formation speaks to Israel's emphasis on intelligence gathering, cybersecurity, and the necessity for solid defensive and offensive cyber capabilities.

These cyber forces are a reaction to the rising understanding that cyber warfare is essential to national and international security. The necessity to secure critical infrastructure-sensitive information and to be able to fight and retaliate against cyber-attacks prompted the creation of these specialist units. Another element driving their development is the ability of cyber operations to carry out strategic objectives without the physical deployment of regular military units.

International Cooperation and Alliances.

In the realm of cyber threats, no nation stands alone. The global nature of these threats necessitates international cooperation and collective defense strategies. Forming or strengthening global cybersecurity alliances is essential. Similar to traditional defense pacts, these alliances would provide platforms for intelligence sharing, joint research and development in cybersecurity, and coordinated responses to significant cyber incidents.

---

[17] "National Cyber Force," GOV.UK, November 17, 2023, https://www.gov.uk/government/organisations/national-cyber-force.
[18] "Unit 8200 – Darknet Diaries," accessed November 29, 2023, https://darknetdiaries.com/transcript/28/.

Since late 2008, NATO has vastly expanded its interest in cyber defense via the NATO Cooperative Cyber Defense Center of Excellence (CCD COE), tasked with researching, developing, training, and educating in the non-kinetic realm of cyber defense.[19] While operating independently, CCD COE has no assigned role in NATO's direct cybersecurity operations; nonetheless, its work is highly influential - especially the publication of the Tallinn Manual, hosting the annual CyCon conference, and large-scale cyber-defense exercise "Locked Shields." These and similar endeavors have all contributed significantly to NATO's ongoing cycle of cyber capabilities buildout.

Another essential step is international cybersecurity standards. These standards would create a common national baseline for cybersecurity measures, providing a more coherent and effective global response to cyber threats. In addition, international legal frameworks and treaties relating to cybercrime and cyber warfare could further promote global cybersecurity governance and cooperation.

Private Sector Engagement and Innovation.

The private sector drives technological innovation and shapes the cybersecurity landscape. Deeper partnerships between governments and technology companies are critical to quickly evolve and introduce advanced cybersecurity solutions. Because of the trends above that are most likely to develop by 2030, initiatives will almost certainly need to include joint ventures to develop AI-driven threat detection systems, use blockchain to enhance security radically and develop next-generation encryption technologies. In addition, governments can be more proactive by encouraging private sector participation in cybersecurity. Whether the best approach is via tax

[19] "CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence Is a Multinational and Interdisciplinary Hub of Cyber Defence Expertise.," accessed November 29, 2023, https://ccdcoe.org/.

incentives, grants, subsidies, or public-private partnership models, including more private investment and innovation in cybersecurity solutions will be vital.

Significant credit for creating groundbreaking technological advances goes to the private sector, and that fact will be an effective force in shaping the cybersecurity landscape. Government and private technology companies must form deeper partnerships to evolve at the velocity required to bring advanced cybersecurity solutions to market. That partnership could take the form of joint ventures to create AI-driven threat detection systems that anticipate and neutralize global-scale cyber threats, utilize blockchain to improve security radically, develop next-generation encryption technologies, and more. Governments can accelerate the process by finding ways to bring private businesses into cybersecurity itself. As with any emerging technology, tax incentives, grants, subsidies, or public-private partnership models could be implemented to ensure that increased private sector investment and innovation in cybersecurity solutions becomes a reality.

The rise of the CCD COE has affected the institutional environment and brought about a surge of cybersecurity-focused startups and well-established tech enterprises in Estonia, solidifying the nation's position as an unequivocal global cybersecurity powerhouse.[20] Cybernetica, BHC Laboratory, Clarified Security, Bytelife, and GuardTime are prominent firms from Estonia highlighted in this context. They symbolize an expanding ecosystem that provides cutting-edge cyber defense solutions and technologies, highlighting the broader ramifications of the CCD COE's inception that extend beyond the immediate jurisdiction of NATO.

Media Collaboration for Public Awareness.

Perhaps the most crucial component of information domain strategy is media collaboration. Partnerships between the media, governments, and cybersecurity experts are necessary to aid in

[20] Harle Pihlak, “How Estonia Became a Global Heavyweight in Cyber Security,” e-Estonia, June 14, 2017, https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/.

educating the public about cyber threats and how best to practice safe cyber behavior. These collaborations could help facilitate public awareness campaigns informing citizens about protecting personal and professional data, recognizing common cyber threats, and practicing cyber-safe behavior. Additionally, these partnerships could offer a means of ensuring that the media reports on cybersecurity issues in a way that debunks myths and accurately assesses one's digital security. In this way, these partnerships could help keep the public informed and vigilant around the clock.

An example of how the media might collaborate to raise public awareness proactively can be found in an advertisement by a Dutch telecommunications company. Dutch Telecom recently showcased a powerful. Recently, Dutch Telecom provided a compelling illustration of the perils associated with deepfakes via an astute media advertisement entitled "A Message from Ella." [21] It gives the audience an excellent example of a deepfake that depicts the speech and movements of a child while being carried out by a deepfake that captures the child's facial expressions and movements exceptionally well. The deepfake effectively replicated the child, Ella, to the extent that her parents were astounded to see a projection of their child on the large screen of a movie theater. Four months after the company uploaded the video to YouTube, it had already amassed more than two million views, demonstrating that this astute and remarkably effective campaign has brought significant public consciousness to the dangers of disinformation made possible by the deepfake technology, which blurs the distinction between fact and fiction. [22]

[21] Deutsche Telekom AG, "'ShareWithCare': Telekom Raises Awareness for Responsible Use of Children's Photos on the Internet," July 3, 2023, https://www.telekom.com/en/company/details/share-with-care-telekom-raises-awareness-1041810.
[22] *Nachricht von Ella | Without Consent*, 2023, https://www.youtube.com/watch?v=F4WZ_k0vUDM.

Conclusion

As it approaches 2030, the future becomes more information-intensive, focusing on information domain complexities. A robust cybersecurity posture requires strategic planning, international collaboration, private-sector innovation, and public outreach. These actions will help nations enhance cybersecurity and provide the framework for future digital security. 2030 may see the information realm as a resource and warfare. Essential for geopolitical maneuvering and national security. Complex and forward-thinking defense solutions are needed to address data breaches and information exploitation, previously peripheral issues. Ultimately, technology, international alliances, and informed individuals determine the future. These initiatives may create a secure and safe digital landscape that dissolves the barrier between the digital and physical, allowing the globe to shrink into a more linked and collaborative community.

Bibliography

AG, Deutsche Telekom. "'ShareWithCare': Telekom Raises Awareness for Responsible Use of Children's Photos on the Internet," July 3, 2023. https://www.telekom.com/en/company/details/share-with-care-telekom-raises-awareness-1041810.

"Alaska Dispatch: China's Cyber Army Is Invading Critical U.S. Services - ProQuest." Accessed January 31, 2024. https://www.proquest.com/docview/2900632176?parentSessionId=hS6OL0K2yAWvijSWJOnplX27m0%2FXuea%2BIerBLfNn0WQ%3D&pq-origsite=primo&accountid=12702&sourcetype=Newspapers.

Borogan, Andrei Soldatov, Irina. "Russian Cyberwarfare: Unpacking the Kremlin's Capabilities." CEPA, September 8, 2022. https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/.

"CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence Is a Multinational and Interdisciplinary Hub of Cyber Defence Expertise." Accessed November 29, 2023. https://ccdcoe.org/.

Dunn, Corey, Nour Moustafa, and Benjamin Turnbull. "Robustness Evaluations of Sustainable Machine Learning Models against Data Poisoning Attacks in the Internet of Things." *Sustainability* 12, no. 16 (January 2020): 6434. https://doi.org/10.3390/su12166434.

GOV.UK. "National Cyber Force," November 17, 2023. https://www.gov.uk/government/organisations/national-cyber-force.

Guadagno, Rosanna E., Karen Guttieri, Rosanna E. Guadagno, and Karen Guttieri. "Fake News and Information Warfare: An Examination of the Political and Psychological Processes From the Digital Sphere to the Real World." Chapter. https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-7998-7291-7.ch013. IGI Global, January 1, 1AD. Fake-news-and-information-warfare. https://www.igi-global.com/gateway/chapter/www.igi-global.com/gateway/chapter/269096.

Haselton, Martie G., Daniel Nettle, and Paul W. Andrews. "The Evolution of Cognitive Bias." In *The Handbook of Evolutionary Psychology*, 724–46. John Wiley & Sons, Ltd, 2015. https://doi.org/10.1002/9780470939376.ch25.

International cyber law: interactive toolkit. "Office of Personnel Management Data Breach (2015)," June 4, 2021. https://cyberlaw.ccdcoe.org/wiki/Office_of_Personnel_Management_data_breach_(2015).

Jinghua, Lyu. "What Are China's Cyber Capabilities and Intentions?" Carnegie Endowment for International Peace. Accessed November 29, 2023. https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734.

JP 3-04 Information in Joint Operations. 4th ed., 2022.

Kaeli, Britt. "How Are Deepfakes Dangerous?" University of Nevada, Reno, March 31, 2023. https://www.unr.edu/nevada-today/news/2023/atp-deepfakes.

Khorram-Manesh, Amir, and Frederick M. Burkle. "Civilian Population Victimization: A Systematic Review Comparing Humanitarian and Health Outcomes in Conventional and Hybrid Warfare." *Disaster Medicine and Public Health Preparedness* 17 (January 2023): e192. https://doi.org/10.1017/dmp.2022.96.

Nachricht von Ella | Without Consent, 2023. https://www.youtube.com/watch?v=F4WZ_k0vUDM.

Niva, Steve. “Disappearing Violence: JSOC and the Pentagon’s New Cartography of Networked Warfare.” *Security Dialogue* 44, no. 3 (2013): 185–202. https://doi.org/10.1177/0967010613485869.

Pihlak, Harle. “How Estonia Became a Global Heavyweight in Cyber Security.” e-Estonia, June 14, 2017. https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/.

Razma, Gintautas. “A Modern Warfare Paradigm: Reconsideration of Combat Power Concept.” *Journal of Security and Sustainability Issues* 8, no. 3 (2019): 435–52. https://doi.org/10.9770/jssi.2019.8.3(12).

Surfshark. “Data Breach Statistics: Q3 2023.” Accessed November 8, 2023. https://surfshark.com/research/study/data-breach-statistics-q3-2023.

“Unit 8200 – Darknet Diaries.” Accessed November 29, 2023. https://darknetdiaries.com/transcript/28/.

U.S. Cyber Command. “CYBER 101 - U.S. Cyber Command Mission.” Accessed November 29, 2023. https://www.cybercom.mil/Media/News/Article/3192016/cyber-101-us-cyber-command-mission/https%3A%2F%2Fwww.cybercom.mil%2FMedia%2FNews%2FArticle%2F3192016%2Fcyber-101-us-cyber-command-mission%2F.

“Why RMAs Still Matter.” Accessed December 13, 2023. https://thestrategybridge.org/the-bridge/2016/1/3/why-rmas-still-matter?format=amp.