Journal of Military and Strategic Studies

VOLUME 22, ISSUE 1

2022 NATO FIELD SCHOOL AND SIM PROGRAM NOMINEE BEST ARTICLE FOR JMSS

Personal Data Exploitation and Social Media Manipulation as a Security Threat for NATO Nations and Democratic Societies

Lauren Mannix

Introduction

Personal data exploitation poses a security threat to NATO not from a technological standpoint in terms of vulnerabilities in its cyber defences but because it is inextricably tied to social media manipulation. The accepted practice of pervasive data collection enables threat actors to weaponize significant volumes of personal data on individuals and groups in targeted influence operations. The intended purpose of these threat actors—both state and non-state—is to undermine civic discourse and democratic processes by exacerbating pre-existing tensions between or among groups and overwhelm online spaces with misinformation and disinformation to drown out legitimate sources. Consequences manifest in the increased radicalization of individuals

ISSN : 1488-559X

and polarization of groups, resulting in increased violence and division in societies. The overarching security challenge is the erosion of trust in democratic institutions, which emboldens and enables autocratic regimes to overthrow previously democratic states. This has significant implications for NATO as an organization that has taken up the mantle of protecting liberal democratic values and supporting allies and partners which are governed by those values at a time when many states around the world continue to edge towards more authoritarian-style government. While data exploitation is a security issue bounded by and carried out with technology, it is not a technological problem by nature. Data exploitation and its application in social media manipulation is the technological-era iteration of psychological warfare, which has been employed by adversarial states since the concept of statehood began. As such, the strategies and techniques required to combat these security threats may be aided by technology, but cannot solely rely on technology for success—a whole-of-society approach is crucial in the mitigation of these threats.

The Implications of Data Exploitation and Social Media Manipulation for NATO

As the world's largest security and defence organization NATO has a critical role to play in communicating the nature and consequences of the security threats related to data exploitation and social media manipulation. In its most recent Strategic Concept (2022) NATO states the central importance of "individual and collective resilience" in carrying out its core tasks to "safeguard our nations, societies and shared values."[1] NATO must dedicate more resources to research in the social sciences to better understand the nature of these security threats beyond a military perspective and develop more robust solutions.[2] To foster resilience NATO must also commit to a higher degree of engagement with citizens and industry to facilitate dialogue with respect to what their roles and stakes are as well as the need for collective effort in combating these threats.[3]

[1] NATO, "NATO 2022 Strategic Concept," *NATO*, (Madrid: NATO, 2022), https://www.nato.int/strategic-concept/.
[2] David Snetselaar et. al. "Knowledge Security: Insights for NATO," *NATO Review*, 30 September 2022, https://www.nato.int/docu/review/articles/2022/09/30/knowledge-security-insights-for-nato/index.html.
[3] David Snetselaar et. al., "Knowledge Security."

The ever-growing presence of misinformation and disinformation online has significantly impacted several NATO nations, which only underscores the need for collective effort in addressing these issues. NATO itself has been the subject of numerous influence operations meant to diminish its legitimacy, weaken confidence in its abilities, and undercut trust in its commitments to provide security and defence to its members and partners. As such, NATO has a vested interest in the research, development, and implementation of solutions to counter the ability of influence operations to leverage data brokers and social media platforms. As an alliance of nations NATO has a significant stake in the countering of data exploitation and manipulation online because its citizens are targeted by influence operations meant to undermine trust in their governments' leadership and erode the liberal democratic values which are the very basis for the political, cultural, and societal cohesion within and among nations of the Alliance.[4] By casting doubt on the legitimacy and effectiveness of democratic governments, autocratic regimes around the world are becoming emboldened to overthrow previously democratic states, causing widespread social and political instability and resulting in the proliferation of human rights abuses and humanitarian crises.[5] This has significant implications for NATO with respect to each of its core tasks, and specifically crisis management, as we are living in a time wherein geopolitical power struggles are characterized by hybrid attacks below the threshold of war which induce states into crisis by stoking internal conflict and instability with manufactured hate speech and falsehoods.[6]

Data Exploitation and the Manipulation Industry

Data is widely considered to be the currency of commerce in today's digital world; in fact, data-driven companies are "nineteen times more likely to be profitable"[7]

[4] Arsalan Bilal, "Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote," *NATO Review*, 30 November 2021, https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.

[5] E. Gyimah-Boadi, "West Africa's Authoritarian Turn," *Foreign Affairs*, 11 July 2022, https://www.foreignaffairs.com/articles/west-africa/2022-07-11/west-africas-authoritarian-turn.

[6] Arsalan Bilal, "Hybrid Warfare."

[7] Henrik Twetman and Gundars Bergmanis-Korats, *Data Brokers and Security: Risks and Vulnerabilities Related to Commercially Available Data* (Riga: NATO Strategic Communications Centre of Excellence, 2021), p. 9, https://stratcomcoe.org/publications/data-brokers-and-security/17.

than their non-data counterparts. Most online platforms collect personal data to be sold to the online advertising industry for legitimate marketing purposes, however, the overzealous collection of personal data on individuals and lack of oversight has resulted in systemic predatory business practices.[8] This is because their business model relies on the profits they make from targeted advertisements displayed on their platforms, and those advertising agencies in turn rely on the personal data collected from the social media platforms they advertise on.[9] This feedback loop provides no incentive for social media platforms to reduce their collection of personal data and it is clear that the exploitation of personal data is the prevailing business model. In addition, online platforms have demonstrated persistent negligence in maintaining appropriate cybersecurity measures[10] which permits illegitimate access to enormous volumes of personal data and enables malicious actors to launch targeted influence operations.

Data exploitation and social media manipulation have created a highly profitable industry purposed with generating inauthentic engagement[11] to increase the likelihood of a social media algorithm picking up and circulating a given piece of content, whether it is an ad for a business trying to sell a product, or a threat actor trying to sell a narrative. The manipulation industry is a massive industry with a global supply chain comprised of hundreds of manipulation "service providers" that service hundreds of thousands of customers around the world.[12] The manipulation industry advertises their services on major search engines such as Google and Bing, which in turn profit from the ad revenue.[13] In the NATO Strategic Communications Centre of Excellence 2021/2022 report on social media platform manipulation it was found that, as an example of the global scope of the manipulation industry, "European service providers rely in

[8] Chris Inglis and Harry Krejsa, "The Cyber Social Contract: How to Rebuild Trust in a Digital World," 12 May 2022, *Foreign Affairs,* https://www.foreignaffairs.com/articles/united-states/2022-02-21/cyber-social-contract.
[9] Pellaeon Lin, "TikTok and Douyin Explained," *Citizen Lab*, 22 March 2021, https://citizenlab.ca/2021/03/tiktok-vs-douyin-security-privacy-analysis/.
[10] Sebastian Bay and Rolf Fredhaim, *Social Media Manipulation 2021/2022: Assessing the Ability of Social Media Companies to Combat Platform Manipulation,* Riga: NATO Strategic Communications Centre of Excellence, 2022, p. 35, https://stratcomcoe.org/publications/social-media-manipulation-20212022-assessing-the-ability-of-social-media-companies-to-combat-platform-manipulation/242.
[11] Bay and Fredhaim, *Social Media Manipulation,* p. 7.
[12] Bay and Fredhaim, *Social Media Manipulation,* pp. 44.
[13] Bay and Fredhaim, *Social Media Manipulation,* pp. 41.

particular on Russian manipulation software and infrastructure providers who, in turn, use contractors from Asia for much of the manual labour required."[14] The social media manipulation industry poses a challenge for NATO for several reasons: there is a low barrier to entry, inadequate cybersecurity measures to prevent unauthorized access, and a lack of regulation and independent oversight allows for predatory practices such as the targeted manipulation of individuals and groups on social media platforms. The global scope of the manipulation industry underscores the need for international collaboration in combating the exploitation of personal data and abuse of online platforms.

Social Media as a Primary Tool of Influence Operations

Social media manipulation in the context of either state-backed or non-state influence operations constitutes the dissemination of misinformation or disinformation in order to sow discord and instability online and offline. These effects are achieved by way of flooding the social media information landscape with enough distorted, false, or misleading information to a target audience to influence their beliefs and opinions on a given topic or cause enough confusion and doubt to discourage them from trusting in other sources.[15] Perhaps it is because so much of our online activity seems inconsequential that we do not afford it the attention and care that we ought,[16] but actors that seek to influence individuals and societies evidently count on that mindset. A single data point may not have much utility, but the sheer volume of data that we produce as we conduct our daily online activities provides a high-resolution portfolio of our interests, education, profession, socioeconomic status, and biases which can be used for exploitative commercial purposes and malicious ones alike.[17] This is especially true for many NATO nations in which there is a high degree of social media use and smart

[14] Bay and Fredhaim, *Social Media Manipulation*, p. 9.
[15] Sanda Svetoka, *Social Media as a Tool of Hybrid Warfare,* Riga: NATO Strategic Communications Centre of Excellence, 2016, p. 11, https://stratcomcoe.org/publications/social-media-as-a-tool-of-hybrid-warfare/177.
[16] Bernadette Kamleitner and Vince Mitchell, "Your Data is My Data: A Framework for Addressing Interdependent Privacy Infringements," *American Marketing Association, Journal of Public Policy & Marketing* 38, no. 4 (2019): p. 443, DOI: 10.1177/0743915619858924.
[17] Twetman and Bergmanis-Korats, *Data Brokers and Security*, p. 9.

technology adoption.[18] The collection and aggregation of the multitude of seemingly inconsequential data that are produced with every online action provides the pattern of an individual's habits and even thoughts[19]—and in the wrong hands it can serve as the guiding framework with which to manipulate an individual or group of people with misinformation or disinformation.[20]

Some of the tools used to augment the reach of influence operations include fake accounts and robotrolls. Fake accounts and robotrolls are automated to circulate inflammatory content meant to get real people who see the content to engage in heated and disrespectful arguments with others online, resulting in increased tensions between groups offline as well.[21] The algorithms of all major social media platforms have demonstrated poor performance in distinguishing between authentic and inauthentic engagement, resulting in inflammatory content getting circulated all the same.[22] Additionally, the inauthentic engagement of fake accounts and robotrolls gives the appearance of "social proof," which deceives people who see it in their social media feed into thinking that others within their social network are engaging with that content.[23] The result is that our deeply ingrained social cues are manipulated into engaging with inflammatory and often fabricated content, while at the same time the reward centres of our brains are being taught to associate expressions of outrage and disgust with the reward of social acceptance.[24] However, research has shown that the reward of online engagement in the form of likes and comments merely activate

[18] Kathy Cao et. al, "Countering Cognitive Warfare: Awareness and Resilience." *NATO Review*. 20 May 2021, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html.
[19] Twetman and Bergmanis-Korats, *Data Brokers and Security*, p. 9.
[20] Bay and Fredhaim, *Social Media Manipulation,* p. 39.
[21] Nitin Agarwal et. al. *Digital Hydra: Security Implications of False Information Online*, Riga: NATO Strategic Communications Centre of Excellence, 2017, p. 7, https://stratcomcoe.org/publications/digital-hydra-security-implications-of-false-information-online/205.
[22] Bay and Fredhaim, *Social Media Manipulation,* p. 7.
[23] Kathy Cao et. al, "Countering Cognitive Warfare."
[24] Galen Druke, "Politics Podcast: Is Social Media Turning Us Into Political Extremists?" *FiveThirtyEight* (blog), 23 September 2022, https://fivethirtyeight.com/features/politics-podcast-is-social-media-turning-us-into-political-extremists/.

temporary dopamine production which fosters patterns of addictive behaviour, without the health benefits of genuine social engagement.[25]

In a study conducted by the NATO Strategic Communications Centre of Excellence on the ability of social media platforms to combat the proliferation of fake accounts and robotrolls on their platforms, it was concluded that the policies and practices of major social media platforms have had no material effect on the manipulation industry.[26] In fact, the study concluded that the manipulation industry is becoming more effective at delivering faster and cheaper manipulation.[27] It appears that rather than posing a threat to their continued operations, social media platforms qualify the abuse of their platforms—and subsequent fines when found accountable—as simply the cost of doing business.[28] Social media algorithms programmed for maximum engagement predispose individuals to addictive behaviours while social media manipulation exposes individuals to a never-ending stream of hate speech and misinformation, creating an environment in which the objectivity of truth and democratic values are under constant attack.[29]

Social Media Platforms as News Sources

The information landscape is becoming more and more enmeshed with social media and content platforms, with more people every year becoming increasingly reliant on their social media to curate their news. Facebook, Twitter, and TikTok are consistently named as go-to sources for news and information and they are the 3rd, 4th, and 19th most trafficked websites, respectively.[30] A significant issue on these platforms, however, is the inability of users to distinguish between what content is factual and

[25] Galen Druke, "Politics Podcast: Is Social Media Turning Us Into Political Extremists?"
[26] Bay and Fredhaim, *Social Media Manipulation,* p. 3.
[27] Bay and Fredhaim, *Social Media Manipulation,* p. 4.
[28] Ian Bremmer, "The Technopolar Moment: How Digital Powers Will Reshape the Global Order," *Foreign Affairs,* 15 September 2022, https://www.foreignaffairs.com/articles/world/2021-10-19/ian-bremmer-big-tech-global-order.
[29] Ulf Ehlert, "Why Our Values Should Drive Our Technology Choices," *NATO Review,* 16 December 2021, https://www.nato.int/docu/review/articles/2021/12/16/why-our-values-should-drive-our-technology-choices/index.html.
[30] Similarweb, "Top Websites Ranking," Accessed 23 September 2022, https://www.similarweb.com/top-websites/.

what is not, and insufficient moderation on platforms to alert users to content that may not be accurate or true exacerbates the issue.[31] The very design of social media platforms poses a challenge for users when determining the authenticity of a piece of news because the design of the social media feed erases the context of any given piece of content—news and information is consumed alongside entertainment and advertisements alike.[32] A lack of reliable moderation and source verification, the erasure of context, and algorithms designed to keep individuals in the "infinite feed" by learning their preferences and serving them similar content adds up to an information environment that inevitably results in a distorted echo chambers bloated with confirmation bias.[33] These challenges are so cognitively demanding of individuals that it becomes prohibitively difficult to determine what information can be trusted and what cannot.

To better understand the security threats posed by the widespread reliance on social media platforms to provide individuals with news, it is useful to contextualize the above insights with regard to how the human brain processes information. In Grolemund and Wickham's study comparing how statistical data analysis relates to human cognitive processes, the authors explain that the human brain comprehends information by using frameworks, or "schemas" [34] (as opposed to hierarchical directories used by computers). In other words, human cognitive processes are far better at understanding a piece of information when it can be associated within a context that relates it to other information. While this allows us to comprehend vast amounts of complex information in a cognitively efficient manner, it also makes us susceptible to discarding or misinterpreting new information that does not fit well within an established schema.[35] Our brains are highly reluctant to update or abandon our schemas and have a tendency to "discredit observations before beliefs whenever it

[31] Bay and Fredhaim, *Social Media Manipulation,* p. 39.
[32] Bravo, Kristina Bravo, "A Little Less Misinformation, a Little More Action," *Mozilla* (blog), 25 August 2022, https://blog.mozilla.org/en/products/teens-gen-z-misinformation-social-media/.
[33] Kathy Cao et. al, "Countering Cognitive Warfare."
[34] Garrett Grolemund and Hadley Wickham, "A Cognitive Interpretation of Data Analysis," *International Statistical Review* 82, no. 2 (2014): p. 188, DOI:10.1111/insr.12028.
[35] Grolemund and Wickham, "A Cognitive Interpretation of Data Analysis," p. 196.

is easy to do so."[36] Oftentimes a direct sensory experience that leaves little room for interpretation is required to initiate closer inspection of a flawed schema.[37]

Data brokers as key providers of data exploitation

Hybrid threats are already notoriously difficult to identify, but the fact that actors with malicious intent are able to operate unimpeded in legally sanctioned commercial markets—the particular markets in mind here being those of data brokers—it is nearly impossible to distinguish between what is legitimate commercial activity and what activity is being conducted by actors with malicious intent.[38] Personal data is collected, aggregated, stored, bought, and sold by data brokers without informed consent, and often without any awareness on behalf of the individual whose personal data is concerned.[39] Data brokers play a central role in the online information space, in which they aggregate personal data on individuals to be sold to advertising companies who then target individuals and demographics for specific products, services, and information.[40] Most, if not all, major data brokers have been hacked at one time or another[41] due to a systemic culture of negligence around proper cybersecurity measures, which expose enormous volumes of personal data to malicious actors who can then weaponize personal data in targeted influence operations.[42]

The discloser of personal data is rarely, if ever, made aware of the identity of the third party in these exchanges, whether it is a single third party or multiple third parties, what personal data in particular is being shared with them and for what purpose.[43] It raises the question whether online platforms suspect that most individuals would likely not be as amenable to the disclosure of their personal data if they knew to

[36] Grolemund and Wickham, "A Cognitive Interpretation of Data Analysis," p. 197.
[37] Grolemund and Wickham, "A Cognitive Interpretation of Data Analysis," p. 197.
[38] James Pamment and Victoria Smith, *Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online*, Riga: NATO Strategic Communications Centre of Excellence, 2022, p. 4, https://stratcomcoe.org/publications/attributing-information-influence-operations-identifying-those-responsible-for-malicious-behaviour-online/244.
[39] Twetman and Bergmanis-Korats, *Data Brokers and Security*, p. 19.
[40] Twetman and Bergmanis-Korats, *Data Brokers and Security*, p. 6.
[41] Twetman and Bergmanis-Korats, *Data Brokers and Security*, p. 20.
[42] Twetman and Bergmanis-Korats, *Data Brokers and Security*, p. 20.
[43] Twetman and Bergmanis-Korats, *Data Brokers and Security*, p. 19.

what extent their personal data was being bought and sold by data brokers.[44] It is precisely because the nature of these online transactions are obscured from viewed—both physically and conceptually—that the capacity of individuals to give true informed consent is severely compromised.[45] Despite the security concerns that arise out of the exploitative collection of personal data, online platforms continue to adhere to this business model because increased data privacy and security ultimately cuts into their bottom line; and yet "unless individuals can protect their own privacy, they lose power."[46] An individual's power in this context may be more clearly defined as that of personal agency, or the capacity of an individual to make their own choices without undue influence.

Current research and future directions

Due to the manifold security threats that arise out of data exploitation and social media manipulation, success in countering these threats is contingent upon a whole-of-society approach.[47] The following section outlines solutions being developed in the private and public sectors alike and which draw on knowledge from a broad range of disciplines. Multidisciplinary and cross-sector collaboration is needed to develop and implement effective solutions and strong leadership is needed to facilitate collaboration, educate and inform stakeholders, and spearhead the adoption of guiding principles and frameworks.

Inoculation theory

Inoculation theory follows the same principles as its epidemiological counterpart, which stipulates that prevention is the cure by way of achieving herd immunity in advance of a viral threat. The NATO Strategic Communication Centre of Excellence report on inoculation theory and misinformation found that rather than

[44] Pamment and Smith, *Attributing Information Influence Operations,* p. 27.
[45] Kamleitner and Mitchell, "Your Data is My Data," p. 443.
[46] Jaron Lanier, "How Should We Think About Privacy? Making Sense of One of the Thorniest Issues of the Digital Age," *Scientific American,* 1 November 2013, https://www.scientificamerican.com/article/how-to-think-about-privacy/.
[47] David Snetselaar et. al., "Knowledge Security."

trying to drown out misinformation with facts, exposing people to a weak strain of a particular manipulative argument prior to a full exposure event served to bolster their psychological resistance.[48] Inoculation proved to be even more effective in combating misinformation when developed with a techniques-based approach as opposed to an issues-based approach.[49] Techniques-based inoculation focuses on manipulation tactics rather than topics, which makes it more effective across the political spectrum because it avoids polarizing issues and instead focuses solely on the methods of manipulation.[50] By exposing the methods, such as "emotionally manipulative language, polarizing language, conspiratorial reasoning, trolling, and logical fallacies,"[51] inoculation fosters psychological resistance against manipulation attempts.[52]

Studies on inoculation theory employed in gamified scenarios to educate people on manipulation techniques has proven highly effective; participants showed marked improvement in their confidence in identifying manipulation and demonstrated increased reluctance to share and spread the manipulative content.[53] The gamification of inoculation provides a highly engaging way for people to learn about manipulation techniques and cultivate the critical thinking skills necessary to protect themselves against manipulation.[54] For these reasons, incorporating the techniques-based gamification approach into school curriculums would be of great value in equipping young people with the tools needed to navigate online information spaces as soon as they begin interacting with them. In settings where the time commitment required of a game is prohibitive, inoculation videos provide a scalable way to implement inoculation—this approach could be incredibly useful implemented as ads during YouTube videos and the like.[55]

---

[48] Jon Roozenbeek and Sander van der Linden, *Innoculaton Theory and Misinformation,* Riga: NATO Strategic Communications Centre of Excellence, 2021, p. 8, https://stratcomcoe.org/publications/inoculation-theory-and-misinformation/217

[49] Roozenbeek and van der Linden, *Innoculaton Theory and Misinformation,* p. 10.

[50] Roozenbeek and van der Linden, *Innoculaton Theory and Misinformation,* pp. 14–15.

[51] Roozenbeek and van der Linden, *Innoculaton Theory and Misinformation,* p. 5.

[52] Roozenbeek and van der Linden, *Innoculaton Theory and Misinformation,* p. 8.

[53] Roozenbeek and van der Linden, *Innoculaton Theory and Misinformation,* p. 14.

[54] Roozenbeek and van der Linden, *Innoculaton Theory and Misinformation,* p. 14.

[55] Roozenbeek and van der Linden, *Innoculaton Theory and Misinformation,* p. 15.

There remains avenues for research into inoculation theory to increase its effectiveness. A few questions that researchers are addressing include how lab performance would translate in real-world settings, what the expected half-life of a dose of inoculation is, whether multiple doses or multiple different inoculation methods would bolster immunity even more than just a single intervention.[56] Perhaps the biggest question for researchers is what proportion of society needs to be inoculated in order to achieve herd immunity.[57]

Just as you do not need to be a mechanical engineer to know how to safely operate a car, you should not need to be a computer scientist to safely navigate the internet. Inoculation theory establishes a framework to educate the public on the dangers present online and provides methods to navigate those dangers. It equips people with the tools needed in order to exercise personal agency and conduct themselves according to their own risk threshold. It is not about keeping people away from the internet but empowering them with the skills necessary to navigate the hazards implicit in a contested information environment so that they can continue to benefit from the best that the internet has to offer.

Data Privacy Policy and Regulation

Many online businesses are built around or heavily rely upon the collection and sale of personal data.[58] This incentivizes predatory business practices and has given rise to the data exploitation and social media manipulation industries. Stronger policy and regulatory frameworks must be developed to curb the aggressive collection of personal data. Policy must clearly communicate to each stakeholder what their respective roles are and regulatory frameworks must demonstrate a zero-tolerance approach to data exploitation. To be effective, policy and regulation must incentivize best practices around data privacy protection and equitably re-distribute risk mitigation so that

[56] Roozenbeek and van der Linden, *Innoculaton Theory and Misinformation,* p. 16.
[57] Roozenbeek and van der Linden, *Innoculaton Theory and Misinformation,* p. 16.
[58] Pamment and Smith, *Attributing Information Influence Operations,* p. 27.

individuals are not disproportionately liable for risks they do not understand and cannot control.[59]

The minimal regulation of data broker markets has proven ineffective at detecting and preventing the ubiquitous practice of data exploitation that underpins the social media manipulation industry.[60] Social media companies are the de facto regulators of their own platforms, which results in conflicting fiduciary duties and business interests. Online platforms have framed the abuses of their platforms as singular events, but the reality is that they are the result of exploiting "systemic flaws in the way their platforms function."[61] Additionally, the fragmentation of a regulatory framework across individual platforms results in different definitions of misinformation, disinformation, inauthentic engagement, and other manipulation techniques which prevents cross-platform comparison of performance in combating platform abuse which in turn prevents insights into what is working and what is not.[62]

A common framework of risk assessment and platform transparency must be developed in collaboration with social media platforms, regulatory bodies, researchers, and independent auditors in order to be able to objectively evaluate risk performance and research and develop effective.[63] Increased transparency and cooperation is needed of online platforms and more clear, consistent language in their treatment of personal data is necessary across online platforms.[64] Independent auditors must also be tasked with evaluating online platforms' performance in adhering to data privacy regulations. Social media and content platforms must work together to develop methods and best practices to combat abuse of their platforms. A coordinated approach is needed in order to better evaluate the performance of platforms relative to one another as an industry at

[59] Chris Inglis and Harry Krejsa, "The Cyber Social Contract."
[60] Twetman and Bergmanis-Korats, *Data Brokers and Security*, p. 19.
[61] Pamment and Smith, *Attributing Information Influence Operations,* p. 27.
[62] Bay and Fredhaim, *Social Media Manipulation,* p. 28.
[63] Hanna Lindbom, *Capability Assessment for StratCom: Using the New Risk Perspective to Inform the Development of Effective Response Capability Assessments for Countering Information Influence Operations*, Riga: NATO Strategic Communications Centre of Excellence, 2022, p. 6, https://stratcomcoe.org/publications/capability-assessment-for-stratcom-using-the-new-risk-perspective-to-inform-the-development-of-effective-response-capability-assessments-for-countering-information-influence-operations/240.
[64] Bay and Fredhaim, *Social Media Manipulation,* p. 39.

moderating content, identifying and removing fake accounts, and combating influence operations and manipulation.[65]

The effects of social media manipulation clearly demonstrate that the privacy of individuals is tantamount to the security of nations. NATO acknowledges data as a strategic asset[66] and as such has a vested interest in its protection. It is of crucial importance for NATO to play to its strengths as a facilitator with influence in terms of what values policy and regulatory frameworks are developed with. By acting as facilitator, NATO can attract like-minded democracies in and beyond the Alliance[67] to tackle the globally distributed threats of data exploitation and social media manipulation and strengthen cooperation among governments. Its central role is not to decide which specific policies are adopted but to influence the values and principles reflected in policy and regulation, supporting collaboration and consultation among like-minded democracies while enabling individual democracies to work within their different cultural, economic, and social realities with a guiding framework.[68]

Privacy-Enhancing Technologies (PETs)

PETs are a broad range of technologies which can employ the power of big data to answer problems that affect whole societies without sacrificing the privacy of individuals.[69] The applications of PETs are diverse across the public and private sectors alike, with applications in healthcare, voting systems, finance, trade, and messaging platforms to name a few.[70]

[65] Bay and Fredhaim, *Social Media Manipulation,* p. 28.
[66] Zoe Stanley-Lockman and Edward Hunter Christie, "An Artificial Intelligence Strategy for NATO," *NATO Review,* 25 October 2021, https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html.
[67] Ulf Ehlert, "Why Our Values Should Drive Our Technology Choices."
[68] David Calvo et. al., "Countering Disinformation: Improving the Alliance's Digital Resilience," *NATO Review,* 12 August 2021, https://www.nato.int/docu/review/articles/2021/08/12/countering-disinformation-improving-the-alliances-digital-resilience/index.html.
[69] Andrew Imbrie et. al., "Privacy Is Power: How Tech Policy Can Bolster Democracy," *Foreign Affairs,* 16 February 2022, https://www.foreignaffairs.com/articles/world/2022-01-19/privacy-power.
[70] Andrew Imbrie et. al., "Privacy Is Power: How Tech Policy Can Bolster Democracy."

Put simply, PETs include a broad range of methods and techniques that protect privacy by enabling an individual to permit to the use of their data in answering a specific question without actually transferring their data or otherwise disclosing it to the party asking the question.[71] In other words, the system abides by the need-to-know basis. This system benefits both parties because it provides the asker of a question with a result without unnecessarily burdening them with the responsibility of protecting vast quantities of personal data and the individual consenting to their data being used to answer a question does not have to worry about their data being illegitimately accessed in a data breach or otherwise exploited.[72]

These technologies dispel the argument that data analysis and data privacy are fundamentally incompatible and require a trade-off.[73] The implications are significant: technology developed with privacy at the centre restores trust among stakeholders of that technology (those whose data is being used and those who are responsible for safeguarding its use), which in turn fosters a more collaborative information and idea-sharing environment that expediates innovation and problem-solving.[74] Privacy as the norm also reduces the threat of data exploitation in that because PETs do not aggregate data on specific individuals, it becomes less profitable for malicious actors to hack into data systems for the express purpose of obtaining and weaponizing large volumes of personal data.

PETs demonstrate that data privacy and technological innovation are mutually strengthening paradigms with as-yet untapped potential for democracies in their ability to foster information sharing for the benefit of the public good without compromising on privacy and security.[75] The development of these technologies requires international forums that can facilitate joint efforts in establishing guiding frameworks and supporting research and innovation.[76] NATO makes for a natural choice in this regard as it already has a proof of concept for the facilitation of international cooperation and

[71] Andrew Imbrie et. al., "Privacy Is Power: How Tech Policy Can Bolster Democracy."
[72] Andrew Imbrie et. al., "Privacy Is Power: How Tech Policy Can Bolster Democracy."
[73] Andrew Imbrie et. al., "Privacy Is Power: How Tech Policy Can Bolster Democracy."
[74] Andrew Imbrie et. al., "Privacy Is Power: How Tech Policy Can Bolster Democracy."
[75] Andrew Imbrie et. al., "Privacy Is Power: How Tech Policy Can Bolster Democracy."
[76] Jared Cohen and Richard Fontaine, "Uniting the Techno-Democracies: How to Build Digital Cooperation," *Foreign Affairs*, 23 November 2021, https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies.

collaboration and possess considerable human and technological capital among its members. NATO and democratic societies are at a critical juncture in the emerging technological era because whoever drives technological advancement will determine what values are embedded and upheld in it.[77]

Conclusion

This paper sought to examine the security threats that personal data exploitation and social media manipulation pose to NATO specifically and democracies broadly. Data brokers and social media platforms each play key roles in the collection, aggregation, and dissemination of personal data on individuals and as such are implicated in the security threats their business practices enable. Data exploitation and data privacy have far-reaching implications for the broader security environment, necessitating a whole-of-society approach facilitated by international leaders who can influence the values and principles adopted into frameworks for problem-solving and solutions. As an international security alliance unified by shared democratic values, NATO makes for a natural leader in this regard. It is crucial to recognize that these are not short-term goals but need to be incorporated into practice at every level, as our societies are only becoming more data-driven and technologically reliant, not less. The importance of collaboration cannot be understated—stakeholders must be encouraged to take initiative for themselves to be able to address specific nuances of their unique environments. NATO and its member nations share a stake in the future of data privacy and online platform transparency, as "Privacy is at the heart of the balance of power between the individual and the state and between business or political interests."[78] In the context of a different geopolitical era marked by a different kind of technological competition, Reinhold Neibuhr expressed in 1949 that "Technical achievements, which a previous generation had believed capable of solving every ill to which the human flesh is heir, have created, or at least accentuated, our insecurity."[79] As Neibuhr observed then, and what remains true today, is that the principle determinant of success

[77] Andrew Imbrie et. al., "Privacy Is Power: How Tech Policy Can Bolster Democracy."
[78] Lanier, "How Should We Think About Privacy?"
[79] Reinhold Niebuhr, "The Illusion of World Government," 1 April 1949, https://www.foreignaffairs.com/articles/1949-04-01/illusion-world-government.

lies not in technological prowess but in the collective strengthening of shared values and common goals.

Bibliography

Agarwal, Nitin, Kiran Kumar Bandeli, Giorgio Bertolin, Nora Biteniece, and Katerina Sedova. *Digital Hydra: Security Implications of False Information Online*. Riga: NATO Strategic Communications Centre of Excellence, 2017. https://stratcomcoe.org/publications/digital-hydra-security-implications-of-false-information-online/205.

Bay, Sebastian and Rolf Fredhaim. *Social Media Manipulation 2021/2022: Assessing the Ability of Social Media Companies to Combat Platform Manipulation.* Riga: NATO Strategic Communications Centre of Excellence, 2022. https://stratcomcoe.org/publications/social-media-manipulation-20212022-assessing-the-ability-of-social-media-companies-to-combat-platform-manipulation/242.

Bilal, Arsalan. "Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote." *NATO Review*. 30 November 2021, https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.

Bravo, Kristina. "A Little Less Misinformation, a Little More Action." *Mozilla* (blog). August 25, 2022. https://blog.mozilla.org/en/products/teens-gen-z-misinformation-social-media/.

Bremmer, Ian. "The Technopolar Moment: How Digital Powers Will Reshape the Global Order." *Foreign Affairs*. 15 September 2022. https://www.foreignaffairs.com/articles/world/2021-10-19/ian-bremmer-big-tech-global-order.

Cadier, Alex, Chine Labbé, Virginia Padovese, Giulia Pozzi, Sara Badilini, Roberta Schmid, Madeline Roache, and Jack Brewster, "WarTok: TikTok is Feeding War Disinformation to New Users Within Minutes — Even if They Don't Search for Ukraine-Related Content." *Misinformation Monitor: March 2022*. *NewsGuard*. Accessed 5 August 2022. https://www.newsguardtech.com/misinformation-monitor/march-2022/.

Calvo, David, Ricky Cheng, Marc Helou, Nyeli Kratz, Claire Liddy, Jolie McDonnell, Tyler Shin. "Countering Disinformation: Improving the Alliance's Digital Resilience." *NATO Review.* 12 August 2021. https://www.nato.int/docu/review/articles/2021/08/12/countering-disinformation-improving-the-alliances-digital-resilience/index.html.

Cao, Kathy, Sean Glaister, Adriana Pena, Danbi Rhee, William Rong, Alexander Rovalino, Sam Bishop, Rohan Khanna, and Jatin Singh Saini. "Countering Cognitive Warfare: Awareness and Resilience." *NATO Review*. 20 May 2021, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html.

Cohen, Jared and Richard Fontaine. "Uniting the Techno-Democracies: How to Build Digital Cooperation." *Foreign Affairs.* 23 November 2021. https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies.

Druke, Galen. "Politics Podcast: Is Social Media Turning Us Into Political Extremists?" *FiveThirtyEight* (blog). 23 September 2022. https://fivethirtyeight.com/features/politics-podcast-is-social-media-turning-us-into-political-extremists/.

Ehlert, Ulf. "Why Our Values Should Drive Our Technology Choices." *NATO Review. 16* December 2021. https://www.nato.int/docu/review/articles/2021/12/16/why-our-values-should-drive-our-technology-choices/index.html.

Frenkel, Sheera. "TikTok Is Gripped by the Violence and Misinformation of Ukraine War." *New York Times.* 5 March 2022 (updated 6 March 2022). https://www.nytimes.com/2022/03/05/technology/tiktok-ukraine-misinformation.html.

Grolemund, Garrett and Hadley Wickham. "A Cognitive Interpretation of Data Analysis." *International Statistical Review* 82, no. 2 (2014): pp. 184–204. DOI:10.1111/insr.12028.

Gyimah-Boadi, E. "West Africa's Authoritarian Turn." *Foreign Affairs.* 11 July 2022. https://www.foreignaffairs.com/articles/west-africa/2022-07-11/west-africas-authoritarian-turn.

Igo, Sarah E. "How Privacy Prevails in the Age of Big Tech." *The Atlantic.* March 2022. https://www.theatlantic.com/magazine/archive/2022/05/privacy-law-technology-california-gajda-seek-and-hide/629373/.

Imbrie, Andrew, Daniel Baer, Andrew Trask, Anna Puglisi, Erik Brattberg, and Helen Toner. "Privacy Is Power: How Tech Policy Can Bolster Democracy." *Foreign Affairs.* February 16, 2022. https://www.foreignaffairs.com/articles/world/2022-01-19/privacy-power.

Inglis, Chris and Harry Krejsa, "The Cyber Social Contract: How to Rebuild Trust in a Digital World," May 12, 2022, *Foreign Affairs,* https://www.foreignaffairs.com/articles/united-states/2022-02-21/cyber-social-contract.

Kamleitner, Bernadette and Vince Mitchell. "Your Data is My Data: A Framework for Addressing Interdependent Privacy Infringements." *American Marketing Association, Journal of Public Policy & Marketing* 38, no. 4 (2019): pp. 433–450. DOI: 10.1177/0743915619858924.

Lanier, Jaron. "How Should We Think About Privacy? Making Sense of One of the Thorniest Issues of the Digital Age." *Scientific American,* 1 November 2013. https://www.scientificamerican.com/article/how-to-think-about-privacy/

Lin, Pellaeon. *TikTok and Douyin Explained*. *Citizen Lab*. 22 March 2021. https://citizenlab.ca/2021/03/tiktok-vs-douyin-security-privacy-analysis/.

Lindbom, Hanna. *Capability Assessment for StratCom: Using the New Risk Perspective to Inform the Development of Effective Response Capability Assessments for Countering Information Influence Operations*. Riga: NATO Strategic Communications Centre of Excellence, 2022. https://stratcomcoe.org/publications/capability-assessment-for-stratcom-using-the-new-risk-perspective-to-inform-the-development-of-effective-response-capability-assessments-for-countering-information-influence-operations/240.

de Montjoye, Yves-Alexandre, Sébastien Gambs, Vincent Blondel, Geoffrey Canright, Nicolas de Cordes, Sébastien Deletaille, Kenth Engø-Monsen, et. al. "On the Privacy-Conscientious Use of Mobile Phone Data." *Scientific Data* 5, article number: 180286 (2018). DOI: 10.1038/sdata.2018.286.

NATO, "NATO 2022 Strategic Concept," *NATO*, (Madrid: NATO, 2022), https://www.nato.int/strategic-concept/.

Niebuhr, Reinhold. "The Illusion of World Government." *Foreign Affairs.* 1 April 1949. https://www.foreignaffairs.com/articles/1949-04-01/illusion-world-government.

Nilsen, Jennifer, Kaylee Fagan, Emily Dreyfuss, and Joan Donovan. "TikTok, the War on Ukraine, and 10 Features That Make the App Vulnerable to Misinformation." *The Media Manipulation Casebook*. 10 March 2022. https://mediamanipulation.org/research/tiktok-war-ukraine-and-10-features-make-app-vulnerable-misinformation.

O'Connel, Mary Ellen. "Data Privacy Rights; The Same in War and Peace." In *The Rights to Privacy and Data Protection in Times of Armed Conflict*, edited by Russell Buchan and Asaf Lubin, pp. 12–28. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2022.

Pamment, James and Victoria Smith. *Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online*. Riga: NATO Strategic Communications Centre of Excellence, 2022. https://stratcomcoe.org/publications/attributing-information-influence-operations-identifying-those-responsible-for-malicious-behaviour-online/244.

Paul, Kari. "TikTok Was 'Just a Dancing App.' Then the Ukraine War Started." *Guardian.* 20 March 2022. https://www.theguardian.com/technology/2022/mar/19/tiktok-ukraine-russia-war-disinformation.

Roozenbeek, Jon and Sander van der Linden. *Innoculaton Theory and Misinformation.* Riga: NATO Strategic Communications Centre of Excellence, 2021. https://stratcomcoe.org/publications/inoculation-theory-and-misinformation/217

Sikder, Orowa, Robert E. Smith, Pierpaolo Vivo, and Giacomo Livan. "A Minimalistic Model of Bias, Polarization and Misinformation in Social Networks." *Scientific Reports* 10, article number: 5493 (2020). https://doi.org/10.1038/s41598-020-62085-w.

Similarweb. "Top Websites Ranking." Accessed September 23, 2022. https://www.similarweb.com/top-websites/.

Snetselaar, David, Georg Frerks, Lauren Gould, Sebastiaan Rietjens, and Tim Sweijs. "Knowledge Security: Insights for NATO." NATO Review, 30 September 2022. *NATO Review*, https://www.nato.int/docu/review/articles/2022/09/30/knowledge-security-insights-for-nato/index.html.

Stanley-Lockman, Zoe and Edward Hunter Christie. "An Artificial Intelligence Strategy for NATO." *NATO Review.* 25 October 2021. https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html.

Svetoka, Sanda. *Social Media as a Tool of Hybrid Warfare.* Riga: NATO Strategic Communications Centre of Excellence, 2016. https://stratcomcoe.org/publications/social-media-as-a-tool-of-hybrid-warfare/177.

Twetman, Henrik and Gundars Bergmanis-Korats. *Data Brokers and Security: Risks and Vulnerabilities Related to Commercially Available Data*. Riga: NATO Strategic Communications Centre of Excellence, 2021. https://stratcomcoe.org/publications/data-brokers-and-security/17.