POLICY INSIGHTS

PIF REPORT

Septemeber 2025

Number 3 | Volume 1

Challenges for Inter-Governmental and Multilevel Governance of the Information Domain and Countering Dis-Information

By
Dave McMahon

About the Policy Insights Forum

The Policy Insights Forum (PIF) is a non-partisan Canadian Think Tank focusing on strategic over-the-horizon public policy issues through independent research, analysis and engagement.

To learn more about the PIF, visit **www.policyinsights.ca.**

Acknowledgments

This publication was written by Dave McMahon, a member of the PIF Selection Committee, has over 35 years of experience in cyber defence, security, and intelligence.

Research Integrity

As a not-for-profit non-governmental organization, the PIF does not adopt or advocate positions on particular matters. The PIF's publications and multimedia productions always represent the views of the author(s) rather than those of the institution. The PIF maintains strict intellectual independence for all of its projects and publications. PIF staff, fellows, volunteers and directors, and those whom the PIF engages to work on specific projects are responsible for generating and communicating intellectual content resulting from PIF projects.

For more information, visit www.policyinsights.ca/intellectual-independence-policy.

Disclaimer

This disclaimer governs the use of this publication. By using this publication, you accept this disclaimer in full. The PIF will not be liable for any business losses, including without limitation loss of reputation, damage to profits, income, revenue, use, production, anticipated savings, current or future business, contracts, commercial opportunities or goodwill. This publication may include copyrighted images or material from a third party. You may need to obtain the copyright holder's permission if you wish to copy or otherwise use copyrighted material. The PIF's activities are governed by the Laws of Canada.

Copyright

This publication may include copyrighted images or material from a third party. You may need to obtain the copyright holder's permission if you wish to copy or otherwise use copyrighted material. For more information, please visit: www.policyinsights.ca/copyright-information.

Limited Print and Electronic Distribution Rights

This publication and trademark(s) contained herein are protected by law. This representation of PIF's intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited. Linking directly to its webpage on policyinsights.ca is encouraged. Permission is required from the PIF to reproduce, or reuse in another form, any of its research products for commercial purposes.

About the PIF Papers

The PIF Papers publish innovative research in the fields of foreign policy, national defence, international development, and intelligence. This series allows industry representatives, academics, and public officials to share innovative ideas and research across Canada and the world. Featuring both established and emerging thought leaders, the PIF Papers aim to bridge gaps and foster greater understanding across the public and private sectors. All PIF Papers are peer-reviewed and reflect the authors' views alone.

The PIF Papers series published two types of manuscripts: Policy Papers and Policy Briefs.

Policy Papers are in-depth research studies of 7000 words or more.

Policy Briefs are focused analyses and commentaries of 2000-7000 words.

The PIF Papers will be published quarterly, but submissions can be sent at any time. Timely pieces can be published more often and sooner.

English submissions should be sent to Philippe Lagassé: pl@samuel.associates.

French submission should be sent to Sarah-Myriam Martin-Brûlé: sm@samuel.associates.

À propos des Études IP

Les Études IP publient des travaux de recherche novateurs dans les domaines de la politique étrangère, de la défense nationale, du développement international et du renseignement. Cette série permet aux représentants de l'industrie, aux universitaires et aux fonctionnaires de partager des idées et des recherches au Canada et dans le monde. Présentant à la fois des leaders d'opinion établis et émergents, les Études IP visent à favoriser un meilleur dialogue entre les secteurs public et privé. Toutes les Études sont évaluées par des pairs et ne reflètent que l'opinion de leurs auteur.e.s.

Les Études IP publient deux types de manuscrits : les Analyses politiques et les Notes politiques.

Les Analyses politiques sont des études approfondies de 7000 mots ou plus.

Les Notes politiques sont des commentaires et résumés plus courts et plus ciblés de 2000 à 7000 mots.

Les Études seront publiées tous les trimestres, mais les soumissions peuvent être envoyées à tout moment. Les articles qui correspondent aux événements de l'actualité ou les soumissions régulières peuvent être publiés plus souvent et plus rapidement.

Les soumissions en anglais doivent être envoyées à Philippe Lagassé: pl@samuel.associates.

Les soumissions en français doivent être envoyées à Sarah-Myriam Martin-Brûlé: sm@samuel.associates.

Table of Contents

About the Policy Insights Forum I
Acknowledgments I
Research Integrity I
Disclaimer I
Copyright I
Limited Print and Electronic Distribution Rights I
About the PIF Papers II
À propos des Études IP II
Sumamry 3
Trends 3
Disinfo America 4
Platforms 4
Governance 5
Emergent Complexity 7
Intergovernmental, multilevel, polycentric governance dimensions of the information domain 7
Cyber Power as the Engine of Misinformation 8
Information Peacekeeping and Cyber Defence 9
From the national to the transnational 10
Coalition-Building 11
DISARM / D-RAIL 12
Countermeasures Framework for FIMI 13
Case Studies 14
Situational Awareness 15
Takedowns, de-platforming, and sanctions: 15
Sanctions: 15
Attributions 15
Deterrence 16
Costs 17
Measurement of Effect (MoE) 17
Conclusion 18

Summary

The framework to counter information manipulation, disinformation and distortion is remarkably similar to what has already been established for cyber security with a notable exception. The information domain is principally owned and operated by the private sector while disinformation is uniquely discovered with open-source intelligence (OSINT) and countered with open effects. Where as industry plays the lead role in cyber defence, civil society is best suited to counter disinformation. Governments are seen as the biggest purveyors of disinformation while industry platforms and the media have a vested interest in amplifying mis-dis-mal-information because it drives revenue through engagement and ad revenue. Therefore multi-stakeholder engagements for countering information manipulation and distortion ought to be built around private sector initiatives supported by public funding and the enforcement of regulatory frameworks for platforms.

Trends

Changing demographics, resource competition, environmental stresses, globalization, economics, governance, urbanization, geopolitics, the unprecedented advancement in science and technology, are significant trends shaping the future environment.

We are in an epoch of converging trend lines and emergent complexity - where evolutionary development is marked by isolated episodes of rapid change between periods of little change - punctuated equilibrium. The asymmetric nature Internet technology, places information and cognitive warfare capabilities in the hands of most nations and non-state actors. Industrial capability is becoming productized and weaponized. Disinformation campaigns can be easily crowd sourced at very little cost, skill or risk.

In the era of strategic competition, the war on truth, will pose the greatest challenge of our lifetime.

Amidst global geopolitical instability, malicious actors (transnational criminal organization, nation states, paramilitary organizations and billionaires) are increasingly using incendiary disinformation to threaten Canadian democratic values and do harm to the Canadian economy.

The chief attack vector for malware is social engineering and deception. Similarly, information manipulation and disinformation campaigns runs over cyber infrastructure. This relationship between cyber and information manipulation is inseparable. Hence, why cyber security solutions involving multi-stakeholder frameworks are directly applicable to countering dis-information.

01 January 1983 is considered the official birthday of the Internet, social media's history began in the mid-1990s and electronic deception is nothing new. The truth is that we have been working on solutions to cyber problems for decades. An international information peacekeeping framework was articulated as early as 1994.

When it comes to FIMI, we have been admiring the problem for some time, and rediscovering solutions when we could swap out the term 'information-threat' for 'dis-information' in cyber security body of knowledge and accelerate progress on the file.

Counter-disinformation strategies can benefit from previous cyber initiatives technology, security, norms of

behavior, privacy, free speech, malicious content filtering net neutrality, legislation and regulatory frameworks. Similarly, FIMI can adopt Frameworks countermining online violence and pathways to radicalization

An ongoing challenge will be aligning regulatory and legal frameworks from cyber security and information space and media broadcast.

Take for example, cyber norms are a framework for responsible state behavior in cyberspace, based on norms developed in the United Nations Group of Governmental Experts (GGE) with the key support and participation of industry, academia and civil society. I would recommend that the community incorporate experience from cyber norms initiatives - but the landscape has shifted pointedly.

Disinfo America

Transitionally, Russian and China operate vast, complex and sophisticated offensive cyber and disinformation ecosystems that are outsourced through decentralized industry proxies making targeting and effects challenging. USA has become a significant source of disinformation affecting the free world

As the United States continues its withdrawal from the center of the rules-based international system, we're witnessing a parallel retreat from its traditional position as the epicenter of global soft power.[1]

The USA has shut down cyber operations against Russia and defunded counter-influence activities under USAID, abolished the Framework to Counter Foreign State Information Manipulation, whilst aligning the administration's narratives with that of Russia and rapidly becoming the greatest source of disinformation affecting the free world. The Record claims that the USA is now the world's leading disinformation factory.

Where once the United States championed a multi-stakeholder vision of the global internet purportedly dedicated to the global good, now, under the transactional "America First" approach, former allies need to contend with the reality that the United States may, at any time, weaponize its dominance of the digital economy. America's technological hegemony represents merely the latest chapter in a long history of leveraging dominance for strategic advantage. [2]

Emboldened by the current US administration, American sources have become the greatest purveyors of disinformation overnight fundamentally changed multinational alliances.

Platforms

Search engines, social media platform owners and telecommunications providers are arguably in the best position to detect and suppress toxic contact form the web through similar Child Safety Initiatives and clean pipes strategies. Although, social media platforms are in best position to stop disinformation, they have created a system that supports disinformation by algorithms and ad revenue by promoting negative content like disinformation.

The Clean Pipes Strategy leverages the power of central telecoms providers to scrub national cyberspace of malicious content. [3]The Canadian Centre for Child Protection (C3P) offers various prevention and intervention services to the Canadian public. Cybertip.ca is owned and operated by the C3P, in partnership with local law

enforcement agencies and the Royal Canadian Mounted Police, whose National Child Exploitation Coordination Centre coordinates and supports national investigations into child sexual exploitation. Today, national telecommunications carriers systematically block Child Sexual Abuse Material (CSAM) material, domains and traffic based on black lists received by independent 3rd party like Canadian Centre for Child Protection (C3P). Never have so many private and public sector institutions willingly aligned to a single purpose as the protection of children. But now AI generated deep fake disinformation apps and content are dominated by the porn industry including child pornography. [4]

The same technical infrastructure put in place at the core of the Internet since 2007 for malware, spam and CSAM could be used for FIMI. Sadly, authoritarian regimes like China have been shaping international standards bodies like ITU as part of Road and Belt Initiative to gain control of the Internet, and have warped the spirit of child safety initiatives to justify the exploitation of dual-use technology towards national censorship programs.

Through the Canadian Security Telecommunications Advisory Committee (CSTAC) the Carriers and Government have sought to establish rules through regulatory symmetry for telecommunications industry. It remains to be seen whether similar symmetric standards and regulations can be applied to social media platforms, search engines and large language models – particularly without USA administration support.

Unfortunately, current US political policy has thrown shade on platform moderation for dis-information and hate speech. Furthermore, the world's richest man uses his platforms X and Grok for the creation and amplification of disinformation, while occupying a key position with the administration. This has forced as recalibration of the FIMI ecosystem, supply-chain, multi-stakeholder alliances, coalitions and partnerships.

When it comes to moderating disinformation, social media platforms have been lowering standards faster then they can be violated.

Governance

Governing and securing the information domain is complex. It is not something one can do unilaterally, nor can it be solved through workshops or policy papers. The solution requires a deep understanding of the issues, a degree of finesse and a whole of society' approach for combating disinformation, toxic content and digital exploitation.

Science is at forefront of this challenge given that it invented the Internet and is now the principal victim of online misinformation. It is important to recognize that many of the challenges we faced decades ago in cyber security, we are now confronting with dis-information. The answers are staring us in the face.

The very nature of the information space and makes it difficult for a single organization to confront on its own. The circumstance of disruptive technology, globalization, multi-level Internet governance and polycentrism [5] break traditional domains-of-control, and entangle private, public, domestic and international levels-of-authority. Knowledge and truth are outside of the scientific domain is relative.

For centuries, territory has been by marked by borders, governed by sovereign states and the rule-of-law. Yet, information is global pervasive, and borderless. It is owned, operated and controlled by the private sector and defined by its digital natives, influenced by market forces and interactions driven by algorithms. Artificial intelligence is playing an even greater role.

"In North America, the Internet is, to a large extent, an unregulated phenomenon, but supported by a regulated infrastructure." [6] Meanwhile, the information domain has undergone dramatic global disruptive changes in the past few years, particularly in highly-contested areas of the network. The "Internet and digital technologies [have] change[d] deeply the economics of regulation and more generally the economics of institutional frameworks." [7] Ad revenue is driven more by content interaction than bandwidth.

History may record our era as one of remarkable naïveté — when nations willingly anchored their digital sovereignty without questioning who controlled its foundations. America's long-standing dominance of the Internet's architecture — once celebrated as a force for innovation and open commerce — is increasingly wielded as a brutalist instrument of national interest.[8]

A quarter trillion dollars in electronic funds transverse the networks in Canada every day. "Some estimates put the economic contribution of the Internet as high as $4.2 trillion in 2016. The Internet of Things (IoT) could result in upwards of $11.1 trillion in economic growth and efficiency gains by 2025. Upwards of one billion new users and 20 billion devices are forecast to be online within five years. To realize its full potential, the Internet of the future will need to be open, secure, trustworthy and accessible to all. Data integrity and veracity of information has become the paramount threat vector onto society. The worst-case scenario is one in which the Internet breaks on our watch"[9] and we lose our grip on the truth.

The battles are no longer over bananas and oil but over the binary architecture of the global economy. Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) have become the new United Fruits — essential infrastructure providers whose services are indispensable to governments, businesses and citizens worldwide. The sovereign territory being contested is not physical but virtual: the cloud environments, communication networks and data repositories where modern economic and political life increasingly unfolds. [10]

There are a couple of characteristics of the information domain that many of us take for granted, but need to think through critically. First, is that online information is a synthetic domain, but with a very real physical and human (social) presence. There is nothing that exists in cyberspace that does not leave a trace, which is quantifiable, capturable, and ultimately, subject to analysis. Second, that data resides, transits, or is created by physical devices that have, both a temporal, and a geographic component. Those three things can be correlated and together create a bordered, territorial domain, even without the imposition or the changes in the governance environment to make it so. The border between human and machine ambient intelligence is eroding. Hence, the Internet-of-Everything.

In 2025, from cloud computing to artificial intelligence (AI), from internet protocols to satellite networks, America's technological supremacy extends into virtually every domain of the information age. Yet what distinguish this form of imperial reach from its historical antecedents is both its ubiquity and its invisibility. Unlike the gunboats of colonial powers or the military bases of Cold War superpowers, America's digital dominance operates largely beyond public view, embedded in the very infrastructure that enables modern economic life. [11]

"The Internet is the first thing that humanity has built that humanity doesn't understand." [12]

Emergent Complexity

The information manipulation, distortion and disinformation are a complex environment. Complex systems, like the information ecosystem, have interacting parts, where the whole is more than the sum of its individual components. It is these interactions that lead to emergent behaviors and patterns that are not readily predictable from the behavior of the individual components alone. The components of a complex system are not independent but interact and influence each other. These systems can self-organize into patterns or structures without a central controller or can spontaneously adapt to changing conditions and environments. Complex systems often have recursive feedback loops, where the output of one part influences the input of another. They often exhibit repeatable self-similar patterns at different scales. The relationships between components in a complex system are often chaotic, non-deterministic and nonlinear, meaning that a small change in one component can have a large impact on the system as a whole – hence the butterfly effect.

A simple meme can affect global security, critical infrastructures or financial markets at the speed-of-light, which are extremely susceptible to rumor. Case in point, one need look no further than tariff tweets sending global markets in trillion dollar free falls.

Intergovernmental, multilevel, polycentric governance dimensions of the information domain

Cyberspace, the information-layer and knowledge-sphere and understanding is a domain where the interests, values, norms and strategy of the Western liberal democratic vision of open networks and freedom, is countered by alternative models posed by states seeking to restrict and control the domain along nationalistic boundaries. These "multipolar politics and the prevailing status quo of strategic ambiguity hinder international cyber regulation." [13] Regulating, establishing and enforcing norms or behavior for dis-mis-mal information is even more abstruse.

There has also been a growing divide between national regulators, international standards bodies, the International Telecommunication Union (ITU), the owner-operators of cyberspace and platform providers. Some of who are global cyber powers in their own right, with more users than countries have citizens. Major social media platforms continue to censor Canadian media and government content as retribution for the federal governments regulation attempts.

Discussions of Internet governance at the ITU have been attentive "to the question of domain names and complex power relationships in a decentralised network structure" [14] as a technical means to regain sovereignty. We now need to consider emergence of models such as polycentrism that "promote self-organization and networking regulations at multiple levels. This bottom-up form of governance is in contrast to the increasingly state-centric approach to both Internet governance and cybersecurity prevailing in forums like the ITU." [15] Governance models using DNS infrastructure, are simply irrelevance in the social media universe – where most disinformation propagates.

The transitional network decentralization "guarantees its reliability, its efficiency and its ability to develop. [The Internet enables] worldwide connectivity that overwhelms existing regulations based on territorial jurisdiction and Government's legitimacy. Digital networks allow bypassing nation-state based regulatory frameworks." [16] This means that "any legislation can be [circumvented] through the Internet because no governmental agency would be able to efficiently supervise the exchanges of information among Internet users under their jurisdiction and

between them and foreign third parties to guarantee the enforcement of existing laws." [17] "The principle of State regulation ... is no longer relevant because the problems they addressed change with the new technologies [that being] intellectual property rights... and convergence." [18] Technological converge in the Internet-of-Everything collapses multiple regulatory silos particularly when one is addressing multi-modal-cross platform misinformation leaving every agency with a vested interest but no one in charge.

The Canadian Security Telecommunications Advisory Committee (CSTAC) was established by Bell Canada in 2010 to support two key Government of Canada initiatives—the National Strategy for Critical Infrastructure and Canada's Cyber Security Strategy. It allows the private and public sectors to exchange information and to collaborate strategically on current and evolving issues that may affect the telecommunications infrastructure, including cyber security threats. The Clean Pipes Initiative in 2010 was architected to filter malicious content from Canadians including spam, malware, child pornography and disinformation, but to date it has not progressed owing to governance issues. This mechanism is suited to regulate mis-information but we are still searching for the arbitrator of truth.

The very definition of cyberspace is evolving faster than out ability to govern it. The information domain is expanding faster than that. Open media, big-data, ubiquitous mobile communications and the IoT are at the centre of national identity and governance. Yet, in many countries around the world, open access to the Internet is Balkanized, blocked, censored, shaped, controlled and denied. The notion of data sovereign is a myth. Social

Cyber Power as the Engine of Misinformation

The centre-of-authority for cyberspace has migrated. It is less about imperial power and more about multinational corporations, non-government organizations, philanthropy, and social agency. Online influence has been led by the marketing, advertising, television and film industry for decades. Control is in the hands of platforms. "This trend toward Internet sovereignty is complicating efforts at enhancing cybersecurity and clarifying governance." [19] However, telecoms regulation at home remains a blunt instrument; far more concerned with tariffs and Canadian media content rather than security, while ignoring complex global issues. Most of the information industry is outside of regulation.

[In the absence of concrete actions from actors across the ecosystem, we could end up in a world where states assert their sovereign control over the network, where private platforms control who benefits from the Internet, or where online criminals dominate the scene. - Global Commission on Internet Governance 2016.

Governments are not the only actor, or even the most significant players in cyberspace or influence. "Analyzing the debate between Internet sovereignty and Internet freedom through the lens of polycentric regulation, provides new insights about how to reconceptualize both cybersecurity and the future of Internet governance."[20]

Western societies rely on infrastructure that is privately owned. Western governments therefore have no choice but to call on the infrastructure's management to perform actions necessary for national goals – from lawful access to cyber security and content moderation. Most of the information infrastructure that Canadians access foreign. There is no Canadian social media platform similar to facebook. Additionally, multinational companies will face conflicting demands from governments, likely made more severe by governments' increasing efforts at extra-

territorial reach. [21] Some platforms and data centres have moved to safe havens, international waters and outer space completely out of the jurisdiction of any country.

The Realpolitik of cyber power is not just about regulatory governance framework. In the evolution of state and civilian cyber power the "oscillation in the balance of power may be peaking, but never before could a dozen people in their pyjamas meaningfully annul the monopoly on the use of force." [22] Similarly, given the asymmetric nature of the information space, a single person like Taylor Swift or Elon Musk has more followers and greater influence than any country. One uses their influence for entertainment, the other politics and propaganda.

There are capabilities now wielded by the private sector for which there is no analog by nations. "The evolving [information] threat, coupled with a lagging regulatory environment, has made the uptake of best practices haphazard. [Furthermore,] governance gaps hamper efforts to collaboratively manage cyber-attacks." [23]

"States increasingly define cyber-territory by where their subjects go, whether by destination control in the Chinese style or by data control in the EU style" [24] but this is old world thinking.

Information Peacekeeping and Cyber Defence

Governments, would be expected to be responsible for protecting public and private assets on the territory of the state from external aggression, but in practice are not unilaterally capable of providing the required protection to citizens in the information domain. Online toxic content (malware and misinformation) targets citizens directly, at scale, bypassing Canada's national security and defence enterprise entirely. The government further isolates themselves from social networks behind corporate firewalls. An information adversary does not need to meet the military on a notional battlefield.

The tensions over information sovereignty have begun to challenge foundational tenets of policy. Nations and corporations are now playing in the same global competitive business markets and a shared risk environment.

The dynamics that shape challenges and relationships between states, and among non-state actors, is not merely evolving but mutating. Public policy needs to consider the complexities that foreign offensive cyber and disinformation introduces into the equation. "Vying national approaches to enhancing [security] can impede multilateral cooperation to secure critical infrastructure"[25]

A cornerstone of the global economy, the information domain is an incubator "for new forms of entrepreneurship, advances in technology, the spread of free speech, and new social networks" [26] that drive economies and express principles. Securing critical information-infrastructure is pivotal.[27] Cyber facilitates disinformation and creates a frictionless slope from competition to conflict while artificial intelligence accelerates creation and propagation of mis-dis-information.

Social media platforms have curtailed their information integrity teams. Data access for researchers has been

restricted or abolished entirely. Meanwhile, artificial intelligence has fuelled cheaper, more sophisticated information manipulation campaigns, long-term, trusted, global partnerships offer the most sustainable defence against rising coordinated threats to democratic information integrity. Large Language Models (LLM) have been shown to be highly susceptible to information manipulation, distortion and hallucination, while some social media platforms and LLMs such as X and Grok, have been identified as principally dis-information platforms themselves.

Thus, countering disinformation through information peacekeeping is challenged by the essentially borderless nature of the Internet and ubiquitous nature of social networks. Governments have been hard-pressed to be at the forefront of this aspect of national [security and] defence by putting in place systems of mutual defence across all sectors of the economy. [28] Attempts at regulation in a complex system like information and truth, is as challenging as regulating the weather.

Misinformation breaks the current siloed regulatory and legal frameworks. Best-practices, policy, programming, regulation, diplomacy and law are simply not ready for this.

That being said, "today's increasingly networked legislators, regulators, diplomats, business and civil society entities need a common mental framework, in terms of shared essentials of governance, and a vision of constitutionalisation, including normative principles, to safeguard both competition and public policy objectives, at a scale congruent to Cyberspace." [29] The same holds true for the information domain in general safeguarding human knowledge.

Operating complex systems require knowing what levers to pull, in what order and measure. "Governments should live up to the challenges of the information society and global networks, but focus on bottlenecks and exercise regulatory self-restraint." [30]

The private sector principally owns, operates and defends the information domain from the underlying infrastructure to hosting the content. Facebook has more users than most countries have citizens. Countering domestic and foreign information manipulation and interference is best lead but independent trusted non-government private sector entities that are supported by both industry and government.

From the national to the transnational

Harnessing insights such as the EEAS' Foreign Information Manipulation and Interference threat assessments, a vital source of insight on transnational FIMI threats, investing in collaborations between fact-checkers such as the European Fact-Checking Standards Network, and strengthening means of sharing insight into malign operations through trusted collaborations such as through the Information Sharing and Analysis Centre (ISAC) and the G7's Rapid Response Mechanism.

Coalition-Building

The Westminster Foundation for Democracy [31] (WFD) suggests that more effective coalition-building, investing in long-term, trusted partnerships of purpose, are the primary means of information responding to the increasing coordination of information manipulators. This means going beyond one-off collaborations and investing in the selfless sharing of resources, the formation of common strategies, and a fresh drive towards cooperation at national and global levels.

Examples of coalitions from WFD that have successfully upheld information integrity:

Ukraine

A coalition of civil society organisations working to fight information manipulation are collaborating to limit duplication and amplify the reach of their work. This grouping of marketers, web traffic analysts, audience segmentation specialists, and narrative researchers are delivering economies of scale, which help them counter Russian manipulation more effectively than any of their organisations could alone.

Kosovo

The independent media outlet The Geopost built a coalition of purpose to plug an unforeseen funding gap. They secured sponsorship from hotels, local business leaders, a restaurant, the diplomatic community, and even a taxi company in what must be one of the most 'whole of society' coalitions the information integrity field has ever assembled.

Philippines

A coalition helped increase message discipline and public confidence in fact-checking. A common challenge for legitimate fact-checkers is the need to avoid confusion with politically biased 'fake fact-checkers.' Civil society duly formed #FactsFirstPH, a coalition which brought together reputable organisations. By adopting a consistent branding for fact-checks across more than 100 legitimate organisations including members of the gold-standard International Fact-Checking Network, #FactsFirstPH was able to consistently signal credibility.

UN Action Coalition on Information Integrity in Elections

In response to calls for meaningful international collaboration on information integrity, the UN Action Coalition on Information Integrity in Elections was created. The grouping recognises that whilst it is placed to see the bigger picture, trust is often rooted locally. Consequently, much of its focus is on galvanising coalitions at the national level.

Taiwan

In Taiwan, organisations recognised that sharing data through trusted coalitions could convert local insight into transnational resilience. Noting that foreign information manipulation and interference (FIMI) campaigns often use similar tactics in different geographies, insight-sharing partnerships were forged with like-minded organisations.

DISARM / D-RAIL[32]

A common means of threat and response categorisation called DISARM was used, alongside STIX (Structured Threat Information Expression), an interoperable open-source language structure. This means of collaboration enabled insight to be acted on in real-time. Canada's Information Integrity Lab at the University of Ottawa is championing the use of DISARM for FIMI mitigation efforts. The private sector in Canada is adopting the DISARM / D-RAIL system [33] that the EU uses to counter FIMI.

The DISARM Framework provides a common language for documenting influence operations to facilitate information sharing within a multi-stakeholder environment. It supports efforts to reduce harms from activities such as 'IO' (influence operations), 'IM'(information manipulation), 'FIMI' (foreign 'IM' and interference), 'FMI' (foreign malign influence) or 'IIO' (illicit influence operations), among other terms and spheres.

Directing Responses Against Illicit Influence Operations (D-RAIL) [34] proposes a strategy shift from combating disinformation to disrupting the infrastructure, funding, and personnel behind Illicit Influence Operations (IIOs). The approach involves five key steps: articulating the IIO's "chain of influence," developing counter-activities to disrupt this chain, continuously monitoring and evaluating both the campaigns and responses, learning and evolving, and ensuring capability and ethical standards.

This strategy relies on interoperability with existing frameworks like the cyber-operations Kill Chain, the DISARM Framework, and the EU DisinfoLab's cost-effectiveness evaluation framework to systematically break down and disrupt IIOs. D-RAIL emphasizes targeting specific illicit operations over general disinformation, thus minimizing the collateral impact on the broader population and aligning responses with democratic values.

Effective implementation of D-RAIL requires diverse capabilities across society, standardization of responses, improved attribution methods, and robust data access and sharing. Ethical considerations are crucial, ensuring responses are necessary and proportional and respecting democratic values without resorting to deceptive tactics. Ultimately, D-RAIL aims to create a more resilient democratic society by making illicit influence operations more difficult, costly, and prone to failure, thereby safeguarding the integrity of democratic institutions and processes.

Countermeasures Framework for FIMI[35]

Countering foreign information manipulation and interference, disinformation and distortion requires the application of measures across the entire kill-chain at four (4) stages of the information channel within a multi-stakeholder environment.

1. Victim/Audience

Building resiliency within the target audience starts with awareness, education, critical thinking and promoting access to authoritative sources of information. Fact-checking, science literacy programs and increased transparency in social media advertising can help the audience make informed decisions. Cyber safe programs substantively reduce exposure to social engineering and disinformation while lowering risk of being harvested as part of a semantic botnet. Counter conspiracy beliefs without challenging a person's identity have been found to be an effective strategy.

2. Message/Payload

The community can tackle toxic messaging and malware with content-based spam and malware filters supported by artificial intelligence (AI), debunking/pre-bunking of posts and suspending accounts of maligned influencers. Counter-narratives are highly-effective but should always be truth-based as part of an information peacekeeping strategy (IPK) or global peace and stabilization operations. Counter-disinformation campaigns require de-confliction by multiple stakeholders between public and private sectors.

3. Infrastructure

Disinformation campaigns rely on cyberspace to propagate and amplify their malicious content or message using social networks, semantic botnets or AI. Cyberspace also offers an effective means to hide through obfuscation and non-attribution networks. Enumerating foreign global disinformation infrastructure requires effective open source intelligence and targeting resources. Protective DNS services like Canadian Shield help limit exposure of Internet users to malicious sites. Ultimately taking down or sink-holing malevolent infrastructures has been a more effective strategy than chasing billions of toxic messages consumed by a target audience after they have already spread and build an organic domestic audience.

4. Actor

The threat actor sits at the top of the food chain. Whether that is a hostile intelligence service (HoIS) or paramilitary or transnational criminal organization, troll farms, person-of-influence or platform owner. Targeting the threat actor requires strong attribution substantiated with sophisticated intelligence, but is worth the effort. Cut the head off the troll and the disinformation campaign goes silent. Effects can include sanctioning

companies and individuals, freezing assets, dismantling financial networks, disrupting command and control, or following through with indictment and prosecution. Industry has been actively disrupting and dismantling adversary networks, exposing and prosecuting actors effectively for quite some time. The importance of persistent engagement at its core is to preserve our advantages and defend national interests in, through and from the information domain by contesting adversaries' malicious activity during day-to-day competition. Strategic advantage is achieved through operations that hunt down the threat, close the attribute chain, defend forward, contest and counter the adversary in real-time. Proactive counter-disinformation operations targeting threat actors have been proven far more effective than pursuing reactive measures cleaning up the downstream effects of a disinformation campaign.

Case Studies

The Doppelganger operation was a quintessential case study of a community-driven, open-source investigation, illustrating how media, civil society organisations (CSOs), platforms, and authorities collaboratively counteract foreign influence and misinformation (FIMI) campaigns. Despite a range of responses from key stakeholders, including sanctions and legal actions, the Doppelganger operation, now in its second year, persists. This necessitates reflecting on the cost-effectiveness of these responses, considering the expertise, time, and financial resources invested by the defender community to disrupt the Russian network.[36]

Doppelganger is a Russian disinformation campaign established in 2022 by Russian IT firm Social Design Agency (SDA). It has targeted Ukraine, Germany, France, and the United States, with the aim of undermining support for Ukraine in Russia's invasion of the country.

The multi-stakeholder campaign to counter Doppelganger is similar to the takedown of the Russian Business Network (RBN) was a multi-faceted cybercrime organization notorious for its hosting of illegal operations. It originated as an Internet service provider for child pornography, phishing, spam, and malware distribution physically based in St. Petersburg, Russia. By 2007, it developed partner and affiliate marketing techniques in many countries to provide a method for organized crime to target victims internationally. Telecommunications carriers and banks effectively took down the RBN in 2009 by sink-holing Internet infrastructure and seizing financial accounts. However, the organization was able to re-constitute on alternative infrastructure. More sophisticated countermeasures including cyber deception operations and legal prosecution were ultimately more effective.

Analysis of the efficacy of countermeasures used in the Doppelganger case are a template for multi-stakeholder engagement in FIMI as outlined by Disinfo.eu:[37]

Situational awareness

Media outlets were the first to disclose the campaign, informing the public about the threat. Civil society organisations soon followed, leading to platform takedowns and attribution. Public institutions were the last to respond, likely due to bureaucratic processes and the need for cautious attribution of foreign interference.

Takedowns, de-platforming, and sanctions:

Have indeed impacted the malign actors' capabilities, causing a deceleration in content production and infrastructure distribution. However, these efforts have led to slowdowns rather than shutdowns. Doppelganger operators have consistently found ways to circumvent sanctions and improve their obfuscation techniques, resulting in even higher proliferation of URLs and ads and possibly new campaigns exploiting the same infrastructure. The defender community has managed to wound but not kill the operation.

Sanctions:

European Union – In July 2023, the Council of the EU imposed restrictive measures against seven Russian individuals and five entities responsible for the Doppelganger/RRN operation (i.e., Social Design Agency, Struktura National Technologies, Inforos, ANO Dialog, and the Institute of the Russian Diaspora). These sanctions include asset freezes, travel bans, and prohibitions on transactions involving the sanctioned entities and individuals.

United States – In March 2024, the USA Department of the Treasury's Office of Foreign Assets Control sanctioned two individuals (Ilya Andreevich Gambashidze and Nikolai Aleksandrovich Tupikin) and two entities (Social Design Agency and Struktura) for providing services to the Russian Federation. As a result, all transactions involving funds, goods (including properties), or services with these individuals and entities are prohibited.

Attribution

Attribution has been achieved despite its challenges and costs. The primary difficulty lies in the lack of standardised information for knowledge sharing among analysts, with some exceptions for reports containing technically advanced forensics. Access to data is crucial for improving platform accountability and transparency, as well as creating more attribution opportunities. The Digital Services Act (DSA) should play a key role in granting researchers access to large-scale platform data, enabling them to study systemic risks in-depth and support research tackling FIMI campaigns.

Similarly, the attribution of Russian Cognitive Warfare activities was successfully addressed under Cyber Attribution of Sophisticated Threat Actors in the Defence of Canada – research sponsored by Innovation for Defence Excellence and Security (IDEaS) of the Canadian Armed Forces. [38] The project completed a target

system analysis of the Wagner group and cognitive warfare operations in Africa. The research demonstrated that attribution is Intelligence-led technology-accelerated target-driven process, and built orchestration around a technology-accelerated solution. The intelligence from the project contributed to identifying attacks, compromises, end-attribution and countering Russian cyber / cognitive warfare activities, including sanctioning of Russian entities by global affairs, US State Department and the International Criminal Court. The initiative effectively partnered with across government, allies, International criminal court, investigative journalists, civil society, community researchers and commercial intelligence community. Disinformation is uniquely discoverable by and countered by open sources and methods. The research project demonstrated the criticality of open and commercial source intelligence (OSINT/CSINT) and leadership role the private sector plays in countering cognitive warfare of nation states and their proxies.

Deterrence

The Doppelganger investigation found that engaging with domain name registries as the intermediary closest to the problem of impersonation is the most effective way to address issues such as impersonation. Legislative grounds such as abusive domain name registration, trademark laws, copyright infringement, identity theft, and cybercrime offer pathways for prosecution. Additionally, the DSA presents potential avenues for enhancing situational awareness, attribution opportunities, reducing distribution, and ultimately deterring FIMI operations.

Legal actions undertaken by he Doppelganger investigation included:[40]

Süddeutsche Zeitung – Between September and November 2022, Süddeutsche Zeitung used ICANN's UDRP (Uniform Domain Resolution Procedure) to bring a case before the WIPO arbitration panel to have the domain sueddeutsche[.]me successfully transferred to the German newspaper.

Le Monde – In July 2023, lemonde[.]ltd was transferred to French newspaper Le Monde via UDRP.

French Ministry of Foreign Affairs – In October 2023, the World Intellectual Property Office (WIPO) ruled that NameCheap, responsible for selling the domain name diplomatie[.]gouv[.]fm should return it to the French Ministry of Foreign Affairs.

Le Parisien – In February 2024, French registry operator AFNIC returned the domain name leparisien[.]re to Le Parisien.

On 30 April, the European Commission opened formal proceedings to assess whether Meta may have breached the Digital Services Act. "The Commission suspects that Meta does not comply with DSA obligations related to addressing the dissemination of deceptive advertisements, disinformation campaigns and coordinated inauthentic behaviour in the EU", the statement reads. Meta's key role in amplifying the Doppelganger campaign is a clear example of such behaviour.

Costs

The Doppelganger investigation concluded that countermeasures can significant costs, drawing from limited organisational budgets in terms of human resources, legal costs, and potential safety risks for researchers. Conversely, the threat actors appear well-equipped with resources and funds, continually adopting new Tactics, Techniques, and Procedures (TTPs) to sustain their operations. Despite the toughest measures, such as sanctions prompted by reports from Viginum and Meta, the Doppelganger infrastructure remains resilient. [41]

Measurement of Effect (MoE)

Countering dis-information requires an established scientifically-sound means for the Measurement-of-Effect (MoE). Everyone must agree on objectives and what winning looks like within multi stakeholder engagement framework. We also need to standardization terms.

Measuring the effect (MoE) and influence of activities requires a structured approach that includes defining desired outcomes, using performance indicators, collecting data, and analyzing results. It's crucial to involve stakeholders, consider both internal and external validity, and recognize the interconnectedness of impact. To expand on these concepts:[42]

Defining desired outcomes and mapping stakeholders includes understanding the theory of change to develop a clear understanding of how the activity will lead to desired outcomes, including intermediate objectives and the means to achieve them and stakeholder mapping which identifies all groups (members, users, funders, partners, etc.) that are likely to be affected by your activity, either directly or indirectly.

Performance Indicators (Metrics) are derived from specific metrics (indicators) that will help assess the effectiveness of the work and the impact it has and stakeholder involvement in defining what success looks like from their perspective, what criteria or standards they have for judging performance, and the priority between different indicators.

Collecting and Analyzing Data related to the chosen indicators and objectives and data analysis of collected data to understand the extent to which the activity is achieving its intended outcomes.

Measuring influence can be challenging and may require a combination of quantitative and qualitative methods, such as brand surveys, social media sentiment analysis, and anecdotal input from client-facing teams. Impact measurement involves assessing the overall effects of your activity, considering both the intended and unintended consequences.

Conclusion

The coming years promise to be messy and unpredictable as the global digital economy fractures from an American-dominated system into a patchwork of regionally aligned networks. [43] Governments must direct investment toward secure, sovereign digital infrastructures, open source intelligence networks and programs while recognizing that counter-disinformation programs are best lead by the private sector. Counter-disinformation and information distortion programs must incorporate measurement of effects supported by quantitative evidence.

When it comes to foreign interference and influence or countermining disinformation and information distortion we have been admiring the problem for quite some time. The next-evolution of human knowledge is not without its risks, opportunities and moral hazards but the solution requires a complete countermeasures framework, adoption of an international intelligence sharing standard, multi-stakeholder engagement strategy, international regulation with teeth and genuine public private partnership.

Endnotes

1 The Secdev Corp

2 The Brutalist Web - America's digital dominance is becoming a geopolitical weapon, Rafal Rohozinski 21March 2025
https://www.cigionline.org/articles/the-brutalist-web/

3 https://www.linkedin.com/posts/ga%C3%A9tan-houle-1005102_securing-a-nation-the-clean-pipe-initiative-activity-7260738961193496577-1_7y

4 Countering AI generated Gender Related Disinformation, a DCCP study by CSKA and SLG, May 2025

5 Polycentrism is the principle of organization of a region around several political, social, financial centres or cyber domains.

6 Ibid. Conflict and good Governance in cyberspace Klaus W. Grewlich

7 Multilevel Governance of the Digital Space. - Eric Brousseau, University of Paris X, Institut Universitaire de France, EconomiX, 27/07/05

8 The Brutalist Web - America's digital dominance is becoming a geopolitical weapon, Rafal Rohozinski 21March 2025
https://www.cigionline.org/articles/the-brutalist-web/

9 Global Commission on Internet Governance 2016

10 The Brutalist Web - America's digital dominance is becoming a geopolitical weapon, Rafal Rohozinski 21March 2025
https://www.cigionline.org/articles/the-brutalist-web/

11 The Brutalist Web - America's digital dominance is becoming a geopolitical weapon, Rafal Rohozinski 21March 2025
https://www.cigionline.org/articles/the-brutalist-web/

12 Google Chairman Eric Schmidt

13 Rex B. Hughes, NATO and Cyber Defence: Mission Accomplished? https://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf

14 Conflict and good Governance in Cyberspace Multi-level and Multi-actor Constitutionalisation, Klaus W. Grewlich

15 Toward Cyber Peace: Managing Cyber Attacks Through Polycentric Governance, American University Law Review, Scott Shackelford, August 20, 2012

16 Ibid. Multilevel Governance of the Digital Space. - Eric Brousseau

17 Ibid. Eric Brousseau

18 Ibid. Multilevel Governance of the Digital Space. - Eric Brousseau

19 Robert K. Knake, Council on Foreign Relations, Internet Governance in an Age of Cyber Insecurity 3 (2010)

20 Ibid. Toward Cyber Peace. Scott Shackelford

21 CSIS 2018 Security Outlook, Chapter 5 – State power and cyber power

22 Chapter 5 – State power and cyber power, 2018 Security Outlook Potential Risks and Threats – Canadian Security Intelligence Service

23 Foundations of Polycentric Governance in Cyberspace, Cyber Attacks in International Law, Business, and Relations: In search of cyber peace. Scott J. Shackelford, Cambridge University Press

24 Ibid. State Power

25 Arie J. Schaap, Cyber Warfare Operations: Development and Use Under International Law, 64 A.F. L. Rev. 121, 141 (2009)

26 Department of Defense Strategy for Operating in Cyberspace, supra, p. 1.

27 Ibid.

28 Ibid. Conflict and good Governance in cyberspace Klaus W. Grewlich

29 Don't Call Us" Governments, Cyber Security, and Implications for the Private Sector Tom Quiggin, Centre for International and Defence Policy, Queens University, 2015, ISBN 978-1-55339-356-6

30 Ibid. Conflict and good Governance in cyberspace Klaus W. Grewlich

31 Westminster Foundation for Democracy
https://www.wfd.org/commentary/strengthen-information-integrity-elections-strengthen-coalitions

32 https://www.disarm.foundation/disinformation
https://www.disinfo.eu/publications/directing-responses-against-illicit-influence-operations-d-rail/

33 https://www.disarm.foundation/disinformation

34 https://www.disinfo.eu/publications/directing-responses-against-illicit-influence-operations-d-rail/

35 www.clairvoyance.network

36 Assessing cost effectiveness responses to the doppelganger-operation By Raquel Miguel, Maria Giovanna Sessa, and Alexandre Alaphilippe https://www.disinfo.eu/publications/assessing-cost-effectiveness-responses-to-the-doppelganger-operation/

37 Assessing cost effectiveness responses to the doppelganger-operation By Raquel Miguel, Maria Giovanna Sessa, and Alexandre Alaphilippe https://www.disinfo.eu/publications/assessing-cost-effectiveness-responses-to-

the-doppelganger-operation/

38 https://www.youtube.com/watch?v=WcdiFUsxDs8

39 Assessing cost effectiveness responses to the doppelganger-operation By Raquel Miguel, Maria Giovanna Sessa, and Alexandre Alaphilippe https://www.disinfo.eu/publications/assessing-cost-effectiveness-responses-to-the-doppelganger-operation/

40 Assessing cost effectiveness responses to the doppelganger-operation By Raquel Miguel, Maria Giovanna Sessa, and Alexandre Alaphilippe https://www.disinfo.eu/publications/assessing-cost-effectiveness-responses-to-the-doppelganger-operation/

41 Assessing cost effectiveness responses to the doppelganger-operation By Raquel Miguel, Maria Giovanna Sessa, and Alexandre Alaphilippe https://www.disinfo.eu/publications/assessing-cost-effectiveness-responses-to-the-doppelganger-operation/

42 https://www.gsdrc.org/docs/open/hdq905.pdf

43 The Brutalist Web - America's digital dominance is becoming a geopolitical weapon, Rafal Rohozinski 21March 2025
https://www.cigionline.org/articles/the-brutalist-web/

About Dave McMahon

Dave McMahon, a member of the PIF Selection Committee, has over 35 years of experience in cyber defence, security, and intelligence. He holds an honours degree in computer engineering from the Royal Military College of Canada and has authored numerous publications throughout his career. Dave has served in senior roles with the Canadian Armed Forces, CSIS, and CSE, and advised Senate committees, the Privacy Commissioner, and intelligence oversight bodies. He is currently CEO of Clairvoyance Cyber Corp and Chair of the Cyber Council for CADSI. Known for his interdisciplinary approach, he applies data science and anticipatory intelligence to address complex security challenges. His work continues to shape policy, industry practices, and innovation in Canada's cyber and defence sectors.