Jean Monnet Module Erasmus+ Civil society in conflict resolution process: the EU experience for Ukraine

101084973 — EURoCoRP — ERASMUS-JMO-2022-HEI-TCH-RSCH

Course “ACTIVISM IN CYBERSPACE AS A HYBRID THREATS COUNTER”

Academic year 2023-2024
Didactic materials

Co-funded by
the European Union

Ostroh Academy
National University

Jean Monnet Module Erasmus+

Civil society in conflict resolution process: the EU experience for Ukraine

101084973 — EURoCoRP — ERASMUS-JMO-2022-HEI-TCH-RSCH

Course

“ACTIVISM IN CYBERSPACE AS A HYBRID THREATS COUNTER”

Academic year 2023-2024

Didactic materials

Co-funded by
the European Union

Ostroh 2024

Course “Activism in cyberspace as a hybrid threats counter”. Academic year 2023-2024. Didactic materials. Ed. Serhii Ishchuk, Tetiana Sydoruk, Dmytro Shevchuk, Olena Shershnova, Kateryna Yakunina. Ostroh 2024. 92 p.

Co-funded by
the European Union

Contents

Project
“Civil society in conflict resolution process: the EU experience for Ukraine”

Project Title: Civil society in conflict resolution process: the EU experience for Ukraine (101084973 — EURoCoRP — ERASMUS-JMO-2022-HEI-TCH-RSCH)

Timing of the Project: 01.11.2022-31.10.2025

Project Coordinator: The National University of Ostroh Academy

About the Project:

This Project aims to promote the EU values of civil society in the conflict resolution process and increase awareness about the present conflicts hybrid type. **Specific objectives** are:

- to activate discussions about current conflicts hybrid type between the academic world and broad audiences, especially media, local policymakers, representatives of amalgamated communities of Rivne and Khmelnytskyi by providing three roundtables with EU speakers;
- to remote excellence in teaching and research in the field of EU studies worldwide by preparation of 3 courses “Hybrid conflicts as a threat to security systems,” “Activism in cyberspace as a hybrid threats counter,” and “Civil society in resolving modern conflicts” (15 ECTS) for not less than 75 BA students;

- to generate knowledge about civil society in the field of conflict resolution process through research activities in this field by preparing 2 peer-reviewed articles;
- to strengthen the role of the EU as a political actor in the conflict resolution process by providing 10 planned project events, especially in Three International Conferences “The problem of cultural identity in the situation of contemporary dialogue of cultures” and the International Conference “Civil society in conflict resolution process: the EU experience for Ukraine” with EU spikers (not less than 200 people will take part);
- to build a stronger project team, who receive the ability to adapt EU experience at local and regional levels for sustainable development of project deliverables, as well as for future ideas and plans;
- to increase the number of information products on the topic of civil society in the conflict resolution process in the project implementation process by creating 3 didactic materials;
- to provide information dissemination and promotion of project activities and results among the citizens of Ukraine by spreading 3 types of this Project's deliverables (website, MOOC and Textbook) to a wider audience.

Course:
“Activism in cyberspace as a hybrid threats counter”

Topic: 1: Hybrid threats in social networks: the realities of the XXI century.

Spreading misinformation through social networks. The activity of fake profiles, their role in propaganda and disinformation. Inciting hatred, and spreading panic through social networks. Official pages of government representatives as a way to combat disinformation. The role of social networks in rallying the public.

Topic 2: Classification of social networks.

Types of social networks: closed; open; mixed Opportunities and disadvantages of open social networks. Functionality of closed and mixed social networks. Global and regional social networks. Personal, professional, and thematic social networks. Division of social networks by types of activity.

Topic 3: Mechanisms of inciting conflicts in social networks.

Functional capabilities of trolls, bots, and electronic armies. Possibilities of infiltration of the circle of friends. Phishing, blackmail, and discrediting. Trade in information. The culture of cancellation. Cyberbullying. OSINT.

Topic 4: Types of information influences.

Manipulation of social consciousness. The effect of monotony, or "social fatigue". Ambivalence as the disorganization of thinking and the production of social anxiety. Desensitization effect.

Topic 5: Infodemia and Information Chaos.

Infodemic is an epidemic in social networks. Spreading fake information and fake news. Popularization of conspiracy theories in social networks. Typical information disorder (information disorder). Manipulation of subjective biases. Information chaos.

Topic 6: Public practice of counteracting misinformation and propaganda.

Development of alertness. Fact-checking. Joint platforms for checking information, and detecting fakes and manipulations. Media regulators and public media in the fight against disinformation.

Topic 7: Media literacy.

The importance of developing digital competencies. Media culture in the information age. Psychological foundations of media literacy. World experience of media education. Electronic literacy. Trans-mediation. Social engineering in social networks.

Topic 8: Development of Soft skills to counter misinformation and propaganda.

Mastering the basics of constructive communication. Ability to conduct difficult negotiations, to persuade. Active listening. Storytelling (the ability to tell). Empathy, emotional intelligence. Positive worldview and ability to adapt to changes. Critical innovative thinking.

Topic 9: European information policy.

The concept and structure of the European information space. Functions and principles of formation and functioning of the European information space. Trans-European component of the European information space, its main components. Strategies and programs for the formation of the European information society.

The main directions of modern information and communication policy of the EU.

Topic 10: Information policy of Ukraine.

Legal support of the state information policy in Ukraine. Institutional support of information policy in Ukraine. Ukraine's integration into the European information space. Foreign political factors influencing the information policy of Ukraine. Information presence of Ukraine in the world. The policy of correction of historical memory as a counteraction to hybression.

Topic 11: Regulatory regulation of information security.

Freedom of expression on the Internet - opportunities and challenges. Information security policy versus information security policy and the sphere of its circulation. Trends in regulatory and legal provision of information security in the EU. Problems of regulatory and legal provision of information security in Ukraine. Information security in the field of human and citizen rights and freedoms. Information and psychological security. Information and technical security.

Topic 12: Anti-disinformation policy: EU practice, implementation in Ukraine.

Countering disinformation: European approaches. Council of Europe standards for countering information chaos (PACE Resolution "Democracy is broken? How to respond?" No. 2326, Recommendation CM/Rec(2018)2, Recommendation CM/Rec(2020)1). European centers for countering disinformation. Center for countering disinformation at the National Security and Defence Council of Ukraine.

Topic 13: EU Disinformation Organization.

European Center of Excellence for Countering Hybrid Threats (Hybrid CoE). European Program for the Protection of Critically Important Information. Hybrid Threats Data Collection Group at the EU Intelligence and Situation Centre. East StratCom Task Force (2015).

Topic 14: Information warfare and operations of influence.

Information war. Social networks as a battlefield. Special information operations (SIO). Acts of external information aggression (FIA). Information terrorism (IT). Information security gap.

Topic 15: Cyberwarfare - threat awareness and counteraction.

Cyberspace as the fifth sphere of warfare. Cyber threats. Cyber-attacks and hacker attacks. Consideration of information technologies (backdoor, DoS attack, direct access attacks). Vulnerable areas of activity.

Topic 16: Attacking information weapon.

Computer viruses. Logic bombs. Means of suppression of information exchange in telecommunication networks, falsification of information in channels of state and military administration. Means of neutralization of test programs. Software errors.

Topic 17: New technologies in mitigating and countering hybrid threats.

Artificial Intelligence. Research and study of new breakthrough technologies. Big Data Analysis.

Topic 18: Information security and cybersecurity.

Principles of information security (confidentiality, availability and integrity). Types of information security (individuals, society, state, information and technical infrastructure). Information influence as a type of information support of the state administration system. Cyber security as a part of information security. Theory and practice of building secure computer systems (system security and design, user security).

Topic 19: Regulatory and Legal Enforcement of Cyber Security in Countries of the European Union: The Experience for Ukraine.

Review of the research on cybersecurity as a component of information security. A legal platform for information security and the protection of cyberspace in developing the economic security of the European Union. Budapest Convention on Cybercrime (Convention On Cybercrime European, 2001). EU Directive on the Security of Network and Information Systems (NIS Directive). EU Cybersecurity Strategy for the Digital Decade (2021). Cybernetic forces are the experience of the world's leading countries.

Topic 20: The vulnerability of cyberspace: Ukraine.

Cyber-dialogue Ukraine and the EU. Cyber security system of Ukraine. The role of public and volunteer organizations in the cyber security system of Ukraine. Cyber security strategy of Ukraine. Legislative consolidation of the main principles of ensuring cyber security of Ukraine.

Teachers

Sergii Ishchuk

Doctor of Legal Sciences, Professor, Director of the Educational and Scientific Institute of Law named after I. Malinovskii of the National University of Ostroh Academy, in 2021 he defended his doctoral dissertation on the topic «Civil society in the context of the European integration of Ukraine: theoretical and legal aspect», he works in the field of research on the legal aspect of civil society.

serhii.ishchuk@oa.edu.ua

http://orcid.org/0000-0002-3080-3870

Tetiana Sydoruk

Doctor of Political Science, Professor, Head of the International Relations Department, Head of the Center for European Studies of the National University of Ostroh Academy, and Researcher of European integration in the context of political crises and hybrid conflicts of the last decade.

tetiana.sydoruk@oa.edu.ua

https://orcid.org/0000-0002-7231-9884

Dmytro Shevchuk

Doctor of Science in the field of Philosophy, Professor, Vice-Rector for Research and Teaching of the National University of Ostroh Academy, specializes in Political Philosophy, and he has experience of participation in the Erasmus+ Programme.

dmytro.shevchuk@oa.edu.ua

https://orcid.org/0000-0001-5609-2600

Olena Shershnova

PhD in Public Administration, Associate Professor at the Journalism and PR-management Department of the National University of Ostroh Academy, she specializes in Public Administration, Media and Communication, she has experience of cooperation with NGOs of Rivne and Khmelnytskii regions, and implementation of EU ideas and values in its regional development strategies, she has experience of participation in the Erasmus+ Programme.

olena.shershniova@oa.edu.ua

https://orcid.org/0000-0003-1582-4515

Kateryna Yakunina

PhD in History, Senior Lecturer at the Philosophy and Cultural Management Department of the National University of Ostroh Academy, she conducts research on the transformation of religious identity in the context of socio-political transformations in recent years.

kateryna.yakunina@oa.edu.ua

https://orcid.org/0000-0002-2948-0429

Reading Texts

Peter Mandaville, Julia Schiwal
A New Approach for Digital Media, Peace and Conflict

As the lines between online and offline behavior continue to blur, peacebuilders need to better understand digital mediums.

Discussions about the negative effects of online communication on society — including its potential to contribute to violent conflict — tend to focus primarily on misinformation and disinformation. The former refers to factually incorrect information that manages to reach audiences at scale, whereas the latter refers to inaccurate information that is spread deliberately and malignantly by some actor or agent in order to produce specific perceptions and outcomes in physical or digital space.

There is also an enduring perception in many quarters that the internet is an inherently liberating and self-organizing medium, one that is separate and distinct from the “real world.” In this narrative, misinformation and disinformation are the bad parts of the good internet. This is a holdover from the early days of the internet when discussions tended to emphasize the internet’s potential for educating and uniting people.

This is an outdated and misleading view of what the internet is today.

For most people today, the internet is not the democratizing force that some hoped it would be during events like the Arab Spring. Rather, most people experience the internet as a rigid, highly organized and closely monitored medium of expression and connection dominated by corporate tech giants and — perhaps somewhat counterintuitively — state actors.

Much of the communication we talk about today as happening on “the internet” (which technically refers to nothing more than a specific protocol for exchanging data between networked computers) actually occurs via a relatively small number of digital platforms (e.g. Discord, TikTok, WhatsApp, Telegram, Instagram, Twitter, Facebook). All of which are governed by algorithms designed to prioritize certain content, shape social interactions and gather data in ways that maximize their commercial potential — a model sharply at odds with most understandings of “community.” These platforms are also increasingly similar to each other, since in order to compete they must each adopt the most effective features of the others — demonstrated through Youtube’s “shorts” feature, which is a close reproduction of Tik-Tok.

Meanwhile, these platforms have grown more pervasive and woven into the rhythms of everyday life, leading to a progressive collapse in the distinctions people draw between different sources of media and information — for many, the lines between “online” and “offline” are getting blurrier.

For example, to many younger people, there is little difference between receiving news in person, through a Discord message or via a meme on Instagram. The emotional, symbolic and psychological weight can be the equivalent regardless of the medium. For those working in the peacebuilding field this insight carries enormous significance for how we think about and classify modalities and causes of conflict stemming from digital mediums.

More specifically, a compelling and up-to-date understanding of violence organized on digital mediums cannot artificially create a divide between “online” spaces and a “real world,” or sharply distinguish "real world communities" from "online communities."

For many, they are one and the same. To understand the evolving relationship between digital communication platforms and violence in a smaller, angrier internet, the peacebuilding field must move beyond such binaries with roots in outdated conceptions of the internet.

The Limit of Misinformation and Disinformation in Peace and Conflict

One particularly well known example of a clear link between digital platforms and violence would be Facebook’s “failure to prevent its platform from being to used to ‘foment division and incite offline violence’” in Myanmar. Military officials in the Southeast Asian nation were behind a systemic campaign to target the Rohingya Muslim minority that resulted in murder, rape and large-scale forced migration.

One solution that has been widely adopted — the use of digital warnings attached to posts flagging them as misinformation or state-sponsored media — can actually serve to deepen suspicion among people already predisposed toward such content. Simply by virtue of being flagged “dangerous or untrue” on platforms assumed to be hostile to any number of groups, such content paradoxically comes to be perceived as “truer” than unflagged content. The flag itself functions to draw attention and heighten excitement over people saying “dangerous things” rather than to neutralize falsehoods or slow the spread of misinformation.

Studies of misinformation and disinformation tend to focus on fact-checking and journalism as natural and obvious solutions to assess and, where appropriate, produce rational and cogent challenges to articulations of political and extremist violence.

The fact-checking approach to misinformation and disinformation comes with stark limitations. The popularization of “post-truth” as a pithy summary of our declining capacity to agree on basic facts and the spread of articles — such as this one — that shift the burden of countering misinformation and disinformation to individuals are symptoms of the failure of this paradigm to account for malignant state, non-state and corporate actors, who collaborate to create rigid, small digital landscapes highly dependent on advertising revenue that financially incentivizes the rapid spread of all information, regardless of its status as misinformation or disinformation.

Misinformation and disinformation are not flaws in the system, they are part and parcel of the fundamental structure of digital mediums. By design, algorithms cannot and do not differentiate information quality. Powerful actors in digital mediums have no incentive to police or remove misinformation or disinformation either, as this would fundamentally undermine the reach and spread of their platforms.

Furthermore, what the misinformation and disinformation framework (and its prescription of fact-checking as remedy) fails to appreciate is that violence organized on digital mediums is as much about group self-expression and identity affirmation as it is about people behaving violently due to incorrect or deliberately false information they find online. People commit acts of violence not simply because they are ill-informed but because they want to hurt people they dislike and find a convenient pretext for doing so.

For example, across the Middle East and North Africa, gender and sexual minorities are targeted by state authorities for posts on social media that simply express who they are without any explicit political content or advocacy. Misinformation and disinformation are not behind this kind of state violence. Even if government authorities hold misconceptions about gender and sexual minorities (in theory “correctable” through exposure to better information), the violence would likely continue because this population is seen as a threat simply by virtue of their identity and is so weak they can be targeted without consequence.

The same holds true for peace activists in many countries around the world: State and non-state actors often perform acts of violence on peaceful protestors based on a wholly accurate understanding of viewpoints they perceive as wrong or dangerous and not in response to rumors and propaganda. This is the point at which the misinformation and disinformation approach, at least in studies of peace and conflict, fails to capture the ways digital media can generate violence.

Expanding our Imagination

As we have been arguing throughout, in many respects our current peacebuilding language falls short of capturing the contemporary digital experience and this is one possible reason our policy prescriptions suffer the same fate. The terminology we use to discuss digital media remains optimistic and often speaks of the consequences of using technology and of technology — when in fact it would be more accurate to say that we live technology in nearly every domain of life, including war and peace.

Some options for improving the peacebuilding field's approach to digital mediums, including the field's response to misinformation and disinformation, among other malignant digital phenomena, include:

Update our understanding of the internet and rapid technology change as a form of "global shock."

The utopian idea of the internet is a long-gone fantasy. The internet is a rigid, tightly controlled, monitored and tracked space. State and corporate actors are powerful and active in intervening across digital communities, for good and ill. The unchecked optimism and artificial barriers we often still assume to exist between the digital and the physical worlds are both gone. We can no longer speak of "online communities" but must rather think in terms of communities with both digital and physical components. Peacebuilding analysis and practice that fails to appreciate this shift will be painfully limited in its capacity to have enduring relevance and offer insight.

Furthermore, many digital spaces that encompass a malignant dimension (such as spreading misinformation and disinformation) often serve more benign and, sometimes highly valuable functions within their communities. Social clubs and gaming or entertainment channels can become sites of recruitment or indoctrination for specific political and ideological agendas and function as platforms for extremist groups to generate financial and material support. The distinction between entertainment and terrorism is far less clear cut than we might think.

Generate better understanding of national and transnational variations in internet cultures and their implications for conflict and peacebuilding.

Across different countries, regions and language groups, we see huge diversity in internet landscapes and cultures of information consumption. Too often, expertise on a country, region or thematic issue, such as gender or religion, underappreciates these variations in digital landscapes. Understandings of such contexts are also often generated from specific user experiences rather than from comprehensive studies of distinctive and often idiosyncratic practices, injecting a degree of bias into research and writing.

In addition, approaches specifically to misinformation and disinformation vary considerable between non-state and state actors and there is only limited research exploring the various strategies adopted by different types of organizations — and even less on effective peacebuilding strategies to counter them. Radical groups may use disinformation to alienate people from society as part of recruitment efforts, meanwhile state actors may use disinformation to harm morale in targeted societies or misdirect enemy resources. These are different tactics, with different strategies, and require different solutions — all of which must move beyond "add truth and stir" to explore new forms of policy, programming and regulation.

Create digital media programming specific to peacebuilding.

Investing in programs and research specifically focused on the role of digital media in peace and conflict can generate the field-specific knowledge and insight necessary to building out new, technology-sensitive approaches to peacebuilding. Ensuring these programs and tools closely track but remain independent of the key digital platforms will be vital to ensuring that they develop an unbiased capacity to assess how corporate, state and non-state actors enable and facilitate violence across digital and physical spaces.

Published:

https://www.usip.org/publications/2023/02/new-approach-digital-media-peace-and-conflict

Review questions:

1. *What is the essence of the negative effect of online communication?*
2. *Describe the place of narratives, disinformation and misinformation on the Internet.*
3. *Name examples when mass protests were organized with the help of the Internet.*
4. *Continue the thought: Today, the intranet is a platform for…*

5. *How do you understand the association: the Internet is a "global shock"?*

Chris Dougherty
Confronting Chaos: A New Concept For Information Advantage

“It failed miserably.” With these words, Gen. John Hyten dropped a bomb on the Defense Department’s vision for fighting China and Russia, the joint warfighting concept. He told a defense industry group that an adversary red team “ran rings around” a U.S. team using the concept in an October 2020 wargame. Some defense thinkers claimed this was no big deal. However, although American teams lose wargames all the time, this is, in fact, a very big deal.

The joint warfighting concept is a top priority for the Pentagon. It’s supposed to align the armed services’ operational thinking and inform future force development. The Defense Department has been developing the concept for years, and yet it still failed. More worrying is why it failed. According to Hyten, the concept assumed U.S. forces could achieve information dominance in a great-power conflict, akin to what the American military attained during the 1991 Gulf War. That assumption is fatally flawed.

Nearly three years after the 2018 National Defense Strategy identified gaining and maintaining information advantage as a critical mission, thinking among Defense Department leadership about information advantage remains muddled. They don’t understand what it means, what it requires, or how to achieve it. This intellectual vacuum permits “zombie ideas” like information dominance to shamble onward while the department and armed services treat technology as a panacea for their operational and strategic headaches.

There’s an exit from this morass. The Pentagon should accept that the post-Gulf War era of imagined U.S. information dominance is over and abandon the idea of connecting “every sensor to every shooter." Instead, it should design its concepts around the fact that degradation, disruption, and disorder are endemic features of warfare and focus on connecting enough sensors to enough shooters under combat conditions. The department should build new networks and data processing technologies, but it should also recognize the critical role of humans in the emerging "techno-cognitive confrontation" with China and Russia. Gaining information advantage requires accompanying new technologies with updated command philosophies, organizational constructs, and training paradigms that will allow U.S. forces to prevail in the chaotic conditions that will characterize great-power conflicts. The alternative is more failure and possible military defeat.

How Did the Defense Department Get Here?

The wargames and analysis that informed the 2018 National Defense Strategy all hammered home the same point: Information and the systems that gather, transmit, store, and process it have become the single biggest vulnerability in putative conflicts with China or Russia. This is the result of three interrelated trends.

First, information technology has become as central to the American way of war as it is to the American way of life. Just as it's difficult to imagine looking for information without Google, it's difficult to imagine mission planning without PowerPoint. Digitization of the force began in earnest in the 1970s, boomed following the Gulf War, and accelerated again after 9/11. Looking at the Gulf War's lopsided outcome and the important roles that information systems and precision-guided weapons played, it's easy to understand why many post-Cold War defense thinkers viewed information dominance as a key source of U.S. operational advantage. But, it became a solution in search of future problems instead of what it actually was: a fleeting phenomenon created by the confluence of U.S. investments, a perfect opponent, and luck.

Second, the collapse of the Soviet Union in 1991, and its replacement in defense planning with regional threats like Iraq and North Korea, shifted the assumptions underpinning the development of U.S. information systems. Rather than designing them to withstand Soviet attacks, the Pentagon built systems with weaker adversaries in mind and those enemies couldn't threaten U.S. systems in space, cyberspace, or the electromagnetic spectrum. The post-9/11 explosion of information systems exacerbated this problem: U.S forces have become increasingly reliant on systems, like satellite communications, that are susceptible to myriad attacks by capable military adversaries. By building an information architecture on the assumption that it is impervious, the Pentagon turned its greatest strength into its most worrying vulnerability.

Beijing and Moscow took note, and the third trend saw their armed forces develop capabilities to attack U.S. information systems as part of their respective strategies to offset American military superiority. In the event of a crisis or conflict with the United States or its allies and partners, China and Russia would seek early advantages by degrading U.S. information systems. They could then achieve their objectives quickly before resolving the conflict on favorable terms. Wargames suggest this is a plausible outcome.

A New Vision, Undefined and Partly Executed

In response to these trends, the 2018 National Defense Strategy prioritized developing a more resilient information architecture and added gaining information advantage to the force-planning construct, which comprises the missions U.S. armed forces collectively need to execute. Lamentably, neither the strategy nor the subsequent Joint Concept for Operating in the Information Environment publicly defined information advantage.

As a member of the team that wrote the defense strategy and one of the people responsible for including information advantage in the force-planning construct, I recall how our team understood information advantage at the time. In contrast to previous technology-focused thinking, information was defined broadly and included technical systems, cognitive processes, and perceptual/psychological effects. The term “advantage” was meant to convey how contested the information environment would be in competition or conflict with an opponent like China or Russia. Unlike “superiority” or “dominance,” with their connotations of decisive or lasting ascendancy, advantage was meant to be marginal, ephemeral, contingent, and constantly fought over.

In sum, information advantage should be understood as gaining a temporary and contested edge in using information through technical systems, cognitive processes, and perceptual/psychological influence to achieve tactical, operational, or strategic advantages against a competitor in peacetime or an adversary in war.

In the absence of any formal definition, the Pentagon has doubled down on building new systems like the joint all-domain command and control architecture. Each service is pursuing its own initiatives within this framework. The Air Force is developing its Advanced Battle Management System. The Army has its Integrated Battle Command System and Project Convergence, while the Navy and Marine Corps have Project Overmatch.

This approach is understandable, but potentially dangerous. While the U.S. military desperately needs a new information architecture to replace its aging patchwork of networks and datalinks, the degree and scope of connectivity these concepts envision is difficult to achieve under benign conditions. They are nearly impossible to realize in the event of a Chinese or Russian attack. Aiming for dominance — rather than advantage — creates unrealistic expectations, warps requirements, and sets these programs up for failure and going over budget. Additionally, by focusing on technology, these initiatives ignore the human aspects of information. China and Russia may target American information systems, but their goal is to degrade U.S., allied, and partner forces cognitively and psychologically. The technical ability to gather and share information is useless without the ability to trust it, convey it to the right audiences, make sound decisions, and take actions based on it.

The Defense Department should simultaneously set less ambitious requirements for its information architecture while expanding the scope of its efforts to gain information advantage.

A New Concept for Information Advantage

Chinese and Russian military writing provides American defense planners some signposts for how to gain information advantage — properly understood — over Chinese and Russian military forces. There are dozens of useful and accessible English sources that summarize Chinese and Russian thinking. Collectively, these sources reveal four approaches that should inform U.S. planning.

First, in the scenarios that most concern American defense planners — like a Chinese invasion of Taiwan or a Russia-NATO conflict — Chinese and Russian political leaders are likely to try to limit the conflict to avoid unwanted expansion or escalation. Second, both states see themselves as locked in a continuous information confrontation or struggle in which they counter U.S. information operations while creating advantageous conditions for themselves. They seek to do this by, among other things, attacking the perceptions of key audiences, like the populations and elites of the United States and its allies and partners, undermining the cohesion of U.S.-led coalitions and potentially endangering U.S. basing access or overflight rights. Third, they plan to attack U.S. and coalition information and command systems early in a conflict —

preemptively if possible. Finally, both Chinese and Russian leaders try to exercise tight, centralized command and control over their armed forces in various ways, including through automation, routinized tactics, and political officers.

A U.S. concept for information advantage should pursue four lines of effort to exploit or counter these Chinese and Russian approaches.

Exploit Tensions Between Active Defense Strategies and Limited Objectives

A key aspect of gaining information advantage — or minimizing disadvantage — early in a conflict is to make China or Russia confront a dilemma of choosing between conflict limitation and escalation control on one hand and operational aggression on the other.

The Defense Department should start creating this dilemma by limiting the effectiveness of reversible and non-kinetic attacks by adversaries, particularly in space. Non-kinetic and reversible attacks carry less risk of escalation than kinetic strikes. Increasing the U.S. space constellation’s resilience to jamming, laser dazzling, or cyber attacks, for instance, would force China and Russia to choose between limiting their space offensives or attacking with kinetic weapons and risking escalation and the creation of debris that might imperil their own constellations or those of neutral parties.

Next, the Pentagon should disperse its information and command systems, which are concentrated at overseas locations like Ramstein Air Base. Dispersing them within the theater would force China and Russia to attack more targets and increase the likelihood that some U.S. systems would survive initial strikes. Spreading systems to more countries also raises the possibility that Chinese and Russian aggression might expand or solidify a U.S.-led coalition.

The United States should also develop an ability to rapidly relocate key overseas functions — like air operations centers — to the homeland. U.S. Central Command recently demonstrated this capability by relocating its Combined Air Operations Center from Qatar to South Carolina. This move took months of planning, but during a contingency combatant commands will need immediately executable options. If critical nerve centers can be relocated quickly, China and Russia would face a dilemma between leaving them unharmed or escalating a conflict by attacking the U.S. homeland. This approach works hand in hand with dispersing key systems overseas. Some functions, like satellite ground stations, should be located forward and should be dispersed. Others, like air operations centers, are such critical targets that relocating them to the homeland is more appropriate.

Increasing multilateral cooperation in critical functions — like space situational awareness —would also confront Chinese and Russian leaders with unwelcome options. They would have to choose between gaining information superiority and expanding a conflict by attacking a critical system on which many countries rely.

Level the Information Playing Field

Peacetime information operations aren’t the Defense Department’s core competence, by either proclivity or legal authority. However, the department is the organization most likely to bear the brunt of failure in the information environment. Gaining information advantage doesn’t necessitate countering every aspect of Chinese and Russian information warfare. Instead, U.S. forces should undertake targeted efforts to build trust with allies and partners to sustain basing access, bolster alliance cohesion, and improve situational awareness. Thankfully, some allies and partners, like Estonia and Vietnam, have proven capable of dealing with Chinese and Russian information warfare. The Pentagon doesn’t need to replicate their capabilities, but rather provide funding, technology, and an ability to disseminate best practices.

The armed services should also educate their personnel about Chinese and Russian information operations and train them on dealing with specific tactics prior to deployment. Once deployed, U.S. servicemembers and units should know that they are in an active information theater, where every action, whether on patrol or off duty, can have strategic ramifications. By aligning their information operations with their real-world operations, U.S. commanders can engender trust in key audiences.

Get Loose

As China and Russia have myriad means to attack U.S. information systems in space, cyberspace, and the electromagnetic spectrum, degradation is inevitable. Instead of trying to ensure information dominance through ubiquitous connectivity, the Defense Department should seek information advantage by being able to operate with degraded systems more effectively than America's opponents.

Operating with degraded systems requires "loose" methods for managing information and executing command, in contrast with the Defense Department's current "tight" command-and-control processes. Tight operations are rigid, hierarchical, methodical, centralized, and exquisitely precise. Loose operations are fluid, flat, omni-directional, improvisational, delegated, and adequately precise. Loose operations should coexist with, rather than replace, tight operations, and U.S. forces should be able to switch between methods as conditions and missions demand. They should get loose when attacking large numbers of armored vehicles in a highly contested and complex targeting environment, for example. But they should be tight when striking a strategic target with a hypersonic missile.

To operate loose, the armed forces should first adopt delegated command models like mission command or command-by-negation. In theory, the armed services already use these methods. In practice, however, command tends toward the "10,000-mile screwdriver." Delegation is the linchpin of loose operations because it enables command with degraded communications, thereby retaining tactical and operational momentum in highly contested environments.

Second, command, control, and communication should be delinked. In tight operations, these functions are combined as "C3," creating a vulnerability whereby adversaries can sever command and control by jamming communications. Instead, command, control, and communications should each function independently. Unity of command would remain, but commanders could issue orders through whichever network is available and delegate control to lower echelons or to other units or services, depending on the mission and conditions.

Third, joint all-domain command and control should be a confederation of smaller networks capable of operating independently, rather than a single super network. The fundamental design principle of this system should be functioning locally when Chinese or Russian attacks degrade long-range connectivity. In that scenario, this federated architecture would retain local connectivity through mobile, ad hoc networks composed of nodes sharing data in multiple directions over short ranges. These short-range mesh networks are difficult to jam and resilient to the loss of individual nodes. Likewise, tactical cloud storage would increase resilience by providing forward forces with access to data without relying on vulnerable high-bandwidth connectivity to rear-area servers. Finally, universal data translators would function like dongles, making different frequencies, waveforms, and data standards mutually comprehensible, thereby allowing data to pass freely across diverse networks including legacy and allied systems. These translators will be crucial for connecting joint or combined forces in contested environments, while also allowing critical information — like command instructions or targeting data — to route around network outages using alternative networks.

The Pentagon is showing progress building this type of system. There's broad agreement about the character of the architecture, and technology demonstrations and experiments show promise. Skeptics note, however, that the consensus is on broad principles and that the devil is in the details. Moreover, technology demonstrations are not major acquisition programs, and funding for these initiatives is inconsistent. These doubts are warranted, but the real cause for concern has to do with these programs' design objectives and requirements: Currently they are too ambitious and emphasize persistent, high-bandwidth, long-range connectivity. Instead, they should focus more on resilience to degradation and disruption. These two objectives are in tension with each other. Attempting to do both could result in incoherence or going over budget.

The final component of loose operations is "good-enough" targeting. The introduction of precision-guided munitions fundamentally altered the role of information in warfare. With the advent of such munitions, information allowed a few weapons to destroy precisely identified and located targets. Counter-terrorism high-value target interdiction represents the apotheosis of this development, with terabytes of exquisite data, collected over weeks, used to target a single person for a drone strike. This deliberate, information- and time-intensive targeting process would be impossible when trying to strike many moving targets in the harried, chaotic, and degraded environments of great-power war. The U.S. military will need to design targeting processes and weapons around information that is "good enough." This requires larger numbers of affordable weapons — like area-effects munitions — as well as smarter weapons, such as the Brilliant Anti-Tank Munition, capable of identifying targets with imprecise initial targeting information.

Organize and Train for Degradation

The 1986 Goldwater-Nichols Act spread a layer of joint frosting on top of a service-dominated cake. Geographic combatant commanders rely on component commanders to plan and execute operations, and component commands align closely with the Air Force, Navy/Marine Corps, and Army. Tensions abound where service interests and responsibilities tangle, like air component commands where every service has assets and demands for support. In wargames, these components often plan independently at the expense of joint priorities. When Chinese or Russian attacks degrade joint communications, each component fixates on its own battle. Rather than achieving synergies, components become less than the sum of their parts.

The ad hoc character of many joint commands exacerbates this problem. Given their roles as de facto military ambassadors, combatant commanders often delegate operational command to joint task forces. Unlike standing combatant command staffs, these commands may not have experience working together, and they may be overseeing unfamiliar rotational forces. The trust and familiarity that are critical for operating in chaotic conditions may be lacking. To remedy this, the Pentagon should create sub-unified commands focused on China (under U.S. Indo-Pacific Command) and Russia (under U.S. European Command). These commands would plan for conflict and oversee standing joint units trained, organized, equipped, and postured specifically to compete with and deter China and Russia.

These shifts would improve integration near the top of the chain of command, but, in a great-power conflict, lower echelons should also work seamlessly across organizational boundaries and operating environments. As communications degrade, tactical commanders lose coordination with joint colleagues and access to capabilities controlled by higher joint headquarters. To address this, the department should “federate” joint commands, pushing them to lower echelons and giving them control of joint capabilities like cyber attacks.

This new operating method requires a new training paradigm that better represents the challenges of operating with degraded systems in contested environments. Given the difficulties involved in incorporating space, cyberspace, and electromagnetic spectrum operations into training ranges, this will require new forms of live, virtual, and constructive training. Wargaming is a cheap and effective tool for preparing personnel — from general and flag officers to junior enlisted — for potential conflict with China or Russia. However, wargame designs need to improve their representation of information challenges to better capture the character of future warfare.

Finally, training should enable the profound inter-service cooperation required by great-power conflict. Current training processes are service oriented, with joint training and exercises generally occurring at the very end of or after deployment. If the department expects units to fight cohesively across services and operating environments, they should train together earlier and deploy together. This is the only way to develop the familiarity and trust needed to execute mission command and delegated control across organizational boundaries.

A Radical Transformation

Information dominance in a conflict with China or Russia is a fantasy. Disruption and degradation are reality. However, this reality presents potential advantages because chaos cuts both ways.

If China or Russia attacks the United States or its allies and partners, it will want to keep the conflict limited and tightly controlled. U.S. forces that can operate effectively after absorbing punches in space, cyberspace, and the electromagnetic spectrum negate the idea of a quick, limited war. American counterattacks, combined with the fog and friction of conflict, will degrade Beijing's and Moscow's detailed operational pictures and disrupt the ability of their leaders to maintain tight control of their armed forces. In this phase of the conflict, the side that can deal with chaos and operate more effectively with degraded systems will likely seize the initiative.

In theory, this is a competition in which professional, highly trained, well-educated, and combat-experienced U.S. forces should excel against Chinese or Russian forces operating under tight, centralized command and control. In practice, however, U.S. forces continue to assume that military advantage is their birthright, rather than something for which they must continually fight. Hyten's comments are a warning to the entire defense community that assuming advantage is a path to defeat. Instead, U.S. forces should become so comfortable operating with degraded information systems in the chaos of combat that China and Russia cannot see a feasible path to victory.

Published:

https://warontherocks.com/2021/09/confronting-chaos-a-new-concept-for-information-advantage/

Review questions:

1. *What is the Joint War Concept?*

2. *What is the strength of the coordinated operational thinking of the armed forces?*
3. *What are “zombie ideas”?*
4. *How can the contradiction between active defence strategies and limited objectives be exploited?*
5. *Could you describe the role of the Information Playing Field?*

Tony Fyler
TikTok acted to quell misinformation on Ukraine

The Chinese-based platform looks responsible in its quest to deliver accuracy.

The US government has a real issue with TikTok. On the surface, that could be attributed to the increasingly Sinophobic stance of US economic policy (with its ever more hardline Anti-Chinese attempts to “rebalance” the semiconductor supply chain), but representatives from both major parties see the social media platform as a threat to US national security, and in December, 2022, it was banned from all government-issue smartphones.

On the surface then, news that in the summer of 2022, 1,704 TikTok accounts were used as part of a pro-Russian network to spread misinformation, disinformation and anti-Ukraine sentiment as a way to influence the way people viewed the illegal Russian invasion of that country, supports the idea that the US government is right to regard TikTok as a potential threat.

A more complex geopolitics.

Except the accounts were targeted towards Germans, Italians and Britons, influencing European (and British) sentiment, rather than impacting the US particularly. There’s arguably some sense there, in that European NATO powers would be the most likely to resist the invasion on their relative doorsteps, and potentially the fastest to supply Ukraine with actual boots-on-the-ground military support. The accounts were aimed at softening resistance among the general public, rather than among leaders or politicians, so the revelations are less supportive of the US government position than they might at first appear.

In a mark of technical sophistication, the accounts used software to spread the pro-Russia, anti-Ukraine propaganda in the local languages of the countries in which they were operating, so as to appeal more easily and directly to that local audience. Depressingly perhaps, the accounts managed to gather more than 133,000 followers before TikTok discovered what was going on.

While it's important to acknowledge that adversarial influencer groups were able to set up over a thousand TikTok accounts and persuade at least 133,000 people to support their content, to sway opinion on matters of crucial geopolitical import, it's also worth noting that in the run-up to events like the UK's Brexit referendum and the 2016 US election, large numbers of voters were swayed by social media propaganda on social media platforms – both before TikTok became the force it is today.

Any available channel.

As such, what we learn is that Putin's Russia particularly will use whatever media exist to spread its propaganda, and that TikTok is not particularly or especially a channel of threat to either national security or social stability on the basis of these accounts.

And then, there's what happened once TikTok had discovered the misinformation and disinformation accounts.

ByteDance, the company that owns TikTok, set about a massive corrective action, specifically to make the information available on the platform more accurate and less prone to the "fake news" of the propaganda accounts. It removed nearly 865,000 fake accounts, which between them had over 18 million followers. Implementing its policy on not allowing impersonation, the company culled nearly 500 accounts based in Poland alone.

That sort of response to the growing evidence of the platform being used as a mouthpiece for pro-Russia propaganda while the country was in the process of invading a neighbor is not naturally in line with the status of a threat to national security.

A trend of responsible governance.

What's more, the response to the realization of the propaganda accounts' existence was not by any means an isolated event. Recognizing a marked increase in attempts by accounts to post political content (in support of the Russian invasion) in the immediate aftermath of the invasion's beginning, the platform began to block Russian (and, in fairness, Ukrainian) advertisers from targeting political ads at users in other European countries.

Seeing a need and a gap in its response, it also hired native-speakers in both Russian and Ukrainian to help moderate the platform's content towards factual accuracy.

And then it began working with Ukrainian reporters to assure its fact-checking process was as accurate as it could be, and set up a digital literacy program to ensure information about the war was factual, restricting access for media outlets with known links to the Russian government, like Russia Today and Sputnik.

Between mid-June and mid-December 2022, TikTok reported that it took down more than 36,500 videos, with 183.4 million views across Europe, on the grounds that they infringed the platform's "harmful misinformation" policy.

The data on TikTok's response to the use of its platform by pro-Russian propaganda accounts was released in a report so that TikTok could comply with the European Union's Voluntary Code of Practice on Disinformation – a code that many of the leading social networks have signed up to.

Future plans on evolving technologies.

Nor is TikTok content to rest on whatever laurels it gained from its response. It explained that in the next few months, it would be updating its policies banning “deceptive synthetic content” – deepfakes, as the rest of the world knows them – particularly in response to the likely wave of generative AIs coming in the wake of ChatGPT. That’s evidence of TikTok trying to get ahead of the next generation of threat and propaganda, as well as dealing with the most recent generation.

While it’s true that none of that will matter to those in the US legislature who see TikTok as a national security threat specifically because ByteDance is based in China, where a provision exists that would allow the government to access any data held by the company – in the event it suddenly decided it wanted it (and that it could command that access without the world, and particularly the US, raising international data security cane about it).

But the report of TikTok’s response to the discovery of authoritarian propaganda on its platform at least looks like the sort of response that should be expected of a social media platform trying to act responsibly on its commitment to accurate information and data stewardship in the 2020s.

Published:

https://techhq.com/2023/02/tiktok-acted-to-quell-misinformation-on-ukraine/

Review questions:

1. *Do you use TikTok?*
2. *What are evolving technologies?*
3. *What is the future of evolving technologies?*

Jon Bateman, Nick Beecroft, Gavin Wilde
What the Russian Invasion Reveals About the Future of Cyber Warfare

Three Carnegie experts examine Ukraine's success in cyber defense and cyber competition going forward.

The war in Ukraine is the largest military conflict of the cyber age and the first to incorporate such significant levels of cyber operations on all sides. Below, Carnegie Endowment experts Jon Bateman, Nick Beecroft, and Gavin Wilde discuss the key insights from their new series, "Cyber Conflict in the Russia-Ukraine War."

What does cyber competition in the war look like so far?

Gavin Wilde: In many ways, February 2022 was the culmination of one of the most long-running and extensive information assaults by one state on another in history. If Ukraine could be considered Russia's testing ground for offensive cyber and information operations—primarily to wage political warfare—since 2014, after this year, it seems fair to consider it the best testing ground for Western assumptions about information weapons in conventional warfare more broadly.

Jon Bateman: Ukraine has faced intense levels of Russian offensive cyber operations since the invasion, but these do not seem to have contributed very much to Moscow's overall war effort. As the war began, Moscow launched what may have been the world's largest-ever salvo of destructive cyber attacks against dozens of Ukrainian networks. Most notably, Russia disrupted the Viasat satellite communications network just before tanks rolled across the border, plausibly hindering Ukraine's initial defense of Kyiv. But no subsequent Russian cyber attack has had visible effects of comparable military significance, and the pace of attacks plummeted after just a few weeks of war.

Although destructive attacks are most attention-grabbing, Russia’s main cyber activity in Ukraine has probably been intelligence collection. Russian hackers have most likely sought to gather data to inform Moscow’s prewar planning, kinetic targeting, occupation activities, influence operations, and future negotiations with Kyiv. However, Russian brutality and incompetence seem to have prevented Moscow from properly leveraging cyber intelligence. Additionally, non-cyber intelligence sources—like imagery, human agents, and signals intercepts—have been more practically useful to Russia.

Nick Beecroft: Ukraine has shown formidable defensive strength and resilience on the physical battlefield, and the same is true in cyberspace. Kyiv’s ability to harness the experience of years of Russian cyber attacks, combined with strong support from Western governments and—crucially—technology companies has allowed Ukraine to deploy cyber defenses at a scale and depth never seen before. But it’s not only the scale of defense that has been impressive. An alliance of competing companies and governments with varying agendas is collaborating and learning together to thwart Russian cyber attacks, driven by a shared sense of outrage at the invasion. This is not to say that Ukraine has won the competition in cyberspace, since Russia could yet launch damaging cyber attacks or exploit networks for valuable intelligence. But the war has demonstrated that cyber defense is not a hopeless cause.

It appears to many that Russian cyber operations were less impactful than expected. Why is that?

Jon Bateman: Russia’s low cyber success was the overdetermined result of many factors, including inadequate cyber capacity, weaknesses in non-cyber institutions, and exceptional defensive efforts by Ukraine and its partners. To meaningfully influence a war of this scale, cyber operations must be conducted at a tempo that Russia apparently could sustain for only weeks at most. Moscow worsened its capacity problem by choosing to maintain or even increase its global cyber activity against non-Ukrainian targets and by not fully leveraging cyber criminals as an auxiliary force against Ukraine. Meanwhile, Russia seems unwilling or unable to plan and wage war in the precise, intelligence-driven manner that is optimal for cyber operations. Ukraine, for its part, has benefited from a resilient digital ecosystem, years of prior cybersecurity investments, and an unprecedented surge of cyber support from the world's most capable companies and governments.

Some other oft-cited explanations, like Russia's poor planning or restraint, are less compelling. Nine months of war have given Russian hackers plenty of time to grasp Moscow's war goals, yet the pace of damaging cyber attacks has fallen, not risen, over time. And with Russian forces working hard to destroy Ukraine's infrastructure and immiserate the populace, it would make no sense for Russian hackers to hold back.

Gavin Wilde: The bar seems to have been set too high on two scores: in the West, because we calibrated our expectations under a context far short of all-out war; and in Moscow, because military strategists calibrated theirs according to a version of war they think they saw in the 1990s to 2000s but was never quite accurate. In both cases, even the most sophisticated cyber and information operations are simply more impactful and resonant in periods of relative peace than they appear to be amid the violence, destruction, and ops tempo of a military campaign. The most advanced military cyber forces are still wrestling with how to effectively integrate them. Russia doesn't appear to have done so thus far.

Nick Beecroft: One somewhat surprising feature has been Moscow's apparent concern to avoid unintended or widespread international impacts through cyber attacks. Past Russian cyber operations had featured global disruption (NotPetya worm), aggressive targeting of massive global networks (SolarWinds breach), and pursuit of political objectives through digital intrusions (U.S. election interference, attempted disruption of the 2018 Winter Olympics). All of these operations were exposed, thwarted, or apparently ran out of control, and it's possible that the Kremlin attaches a high risk of unintended or negative consequences to cyber operations against foreign targets outside of the war zone.

The attack against Viasat early in the war, which caused apparently unintended disruption to communications across Europe, may have further undermined the confidence in controlling the effects of cyber attacks. October's ransomware attacks against transportation targets, which included some in Poland, could be an indicator of limited-scale experimentation with achieving targeted effects against countries supporting Ukraine. The stakes are much higher since the invasion of Ukraine raised the specter of direct conflict with NATO, and the Kremlin may simply not trust its cyber agencies to achieve carefully calibrated effects within a strategy of deterrence and escalation.

How might Russia adapt in cyberspace moving forward?

Gavin Wilde: I think the question now is one of how to sustain momentum with much less. The exodus of Western tech from the market means Russian state actors may now be running against the clock before they begin either incurring significant technological debt—lack of necessary hardware to software updates that are not forthcoming—or resorting to the less-trusted Chinese variants. Over time, this could diminish the security and functionality of everything from domestic telecommunications (and thus, surveillance) infrastructure to the high-tech research organizations that develop sophisticated cyber exploits. Meanwhile, Moscow is likely going to deal with a rapidly diminishing pool of R&D funding and especially tech talent—much of which, by all reports, has begun seeking more hospitable homes in places like Georgia, Kazakhstan, Turkey, and Israel. In the near term, I'd expect to see a doubling down on disposable, disruptive-but-not-decisive exploits like wipers that delete data from infected targets.

Jon Bateman: As the war continues, Russian intelligence collection probably represents the greatest ongoing cyber risk to Ukraine. Conceivably, Russian hackers might still have larger impact if they can collect high-value intelligence that Moscow then leverages effectively. For example, the hackers might obtain real-time geolocation data that enable the assassination of President Volodymyr Zelenskyy or the timely and accurate targeting of Ukrainian forces, particularly those with high-value Western weapons systems. Russia might also conduct hack-and-leak operations revealing sensitive war information to the Ukrainian and Western public, such as Ukraine's combat losses, internal schisms, or military doubts. Or it could collect valuable information about Kyiv's perceptions and intentions that can aid Moscow at future talks, among other scenarios. Damaging Russian cyber attacks pose a less serious threat, though they could multiply if Moscow directs more of its overall cyber capability toward Ukraine (at the cost of other objectives) or better leverages cyber criminals.

What are the implications for competition in cyberspace beyond this war?

Nick Beecroft: The war has exposed the huge role of the private sector in defending digital networks at national scale. Commercial entities have morphed from vendors to vital agents of defense and foreign policies. This tends to raise different priorities among the

Western allies. In the United States, the concern is whether the ad hoc coalition deployed to defend Ukraine could be replicated elsewhere, particularly against a Chinese threat to Taiwan. In Europe, there is some unease at the prospect of relying on a “cyber umbrella” provided by a handful of U.S. corporations. Both perspectives encounter similar unanswered questions concerning funding and sovereignty.

Thus far, numerous corporations have been willing to provide a substantial commitment of proprietary services to Ukraine free of charge, but that cannot be sustained indefinitely and may not extend to other situations. Furthermore, the pivotal role of commercial (usually American) actors presents democracies with a challenge of retaining control of foreign and defense policies: governments will need to clarify when and how they could call on private sector capabilities and when and why they might not be available. The invasion of Ukraine sparked a unity of purpose among diverse actors that may not be present in the next conflict.

Gavin Wilde: Russian President Vladimir Putin in September tasked his foreign intelligence service with aiding Russia’s technological development amid economic isolation from the West and recently signed a federal budget in which 30 percent is dedicated to military and security forces. Meanwhile, the war has underscored the central role that precision—from targeting to guidance—will likely play in future conflict. That will require advanced chips, electronic and drone warfare capability, and air defense enhancements. In this regard, Western cyber defenses in the defense industrial complex and their related export controls will likely need to complement each other at unprecedented levels.

Jon Bateman: Russia’s experience suggests that damaging cyber operations can be usefully concentrated in a surprise attack or other major salvo, but they risk fading in relevance during larger, longer wars. To sustain wartime cyber attacks at meaningful levels, militaries may need to build much bigger cyber forces, develop much faster regeneration capabilities, and experiment with short bursts of intense cyber attacks (ideally coordinated with kinetic operations) followed by periods of stand-down. Cyber commands that cannot do these things should probably prioritize cyber defense and intelligence collection in wartime, while reserving cyber attacks for more selective use in peacetime, gray zone, or prewar conditions. Cyber intelligence collection has significant potential to support a variety of wartime military tasks, but this probably depends on having competent analysis and decisionmaking processes and a reasonably precise "way of war."

To be sure, the Ukraine war is just one of many relevant case studies. Militaries with high capability, professionalism, and readiness in both cyber and kinetic disciplines—such as the United States and Israel—have previously leveraged cyber operations to enable strikes on high-value targets. Yet even top-tier militaries seem to have the greatest cyber successes in tightly circumscribed contexts. Overall, the scale of war appears inversely correlated with the strategic impact of cyber operations. If this correlation holds, cyberspace should probably not be seen as a "fifth domain" of warfare equivalent in stature to land, sea, air, and space.

Published:

https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667

Review questions:

1. *What does cyber competition in the war look like so far? Your answer.*
2. *It appears to many that Russian cyber operations were less impactful than expected. Why is that? Your answer.*
3. *How might Russia adapt in cyberspace moving forward? Your answer.*
4. *What are the implications for competition in cyberspace beyond this war? Your answer.*

Maj YuLin Whitehead
Information as a Weapon. Reality versus Promises

We cannot expect the enemy to oblige by planning his wars to suit our weapons; we must plan our weapons to fight war where, when, and how the enemy chooses.

—Vice Adm Charles Turner Joy (1895-1956)

The instruments of battle are valuable only if one knows how to use them.

—Ardant du Picq, Battle Studies

*Special thanks to Dr. Daniel J. Hughes, professor of military history, Air War College, and Maj Mark J. Conversino, professor of airpower history and theory, School of Advanced Airpower Studies, for their invaluable advice and guidance in the writing of this article. Also, thanks to my husband, Ray, for his constant love and support.

THERE ARE MANY views of what con-stitutes information warfare (IW). The differences in interpretation are understandable given the subtle (and sometimes not-so-subtle) variations in the defi-nitions of IW. Also, the various terms used as substitutions for IW add to the differing views of the topic. The differences in interpre-tation have translated into a virtual explosion of literature written by authors with their own definitions of IW.

The literature may be grouped into two broad categories based on the authors' the-matic approach to IW. The first category in-volves a concept that discusses IW in terms of the more traditional notion of the use of "information warfare" to support decision making and combat operations. This first theme does not address the question of whether information is a weapon and is there-fore inappropriate for this article. On the other hand, the second category is a wholly different approach and one that directly pro-vides evidence to support or refute the ques-tion of whether information is a weapon. Authors in this category regard “information as a weapon” in warfare.

Dr. George J. Stein, a professor at the US Air Force’s Air War College, also sees a clear separation between using “information in warfare” and using “information as a weapon” or what he terms *information warfare* or *information attack*.1 He believes that there is significant difference between the two categories. Specifically, he explains information in warfare as all those papers and briefings that begin “Information has always been central to warfare . . .” and then go on to explain that “our new computer system will get information to the warfighter” so he can “achieve information dominance on the battlefield” and thus demonstrate our service’s mastery of IW, confuse information-in-war with information warfare. Whether we are digitizing the cockpit or digitizing the battlefield, this is not IW.2

The US Air Force document *Cornerstones of Information Warfare* makes a similar distinction by distinguishing the difference between *information age warfare* and *information warfare*. It explains the former as “us[ing] information technology as a tool to impart our combat operations with unprecedented economies of time and force,”3 such as cruise missiles exploiting information age technologies to put a bomb on target. Information warfare, however, “views information itself as a separate realm, potent weapon, and lucrative target”4 and fits in the category of using information as a weapon.

Using this typology, it appears many of those who claimed Operation Desert Storm was an information war are actually describing the use of information in warfare or information age warfare.5 For example, Alan D. Campen, a former undersecretary of defense for policy, states that “this war differed fundamentally from any previous conflict [and] the outcome turned as much on superior management of *knowledge* as it did upon performances of people or weapons.”6 Further, using this definition, he and others argue that Operation Desert Storm was not only an information war, but the first one in history. This argument holds little credibility because it was not the first time an armed force failed to attain victory for lack of knowledge.7

The USAF and Dr. Stein’s categorizations of the use of “information as a weapon” and “information in warfare” provide a logical method to separate the two main themes of information warfare literature. However, it is not the author’s intent to argue the merits or faults of their delineations. Rather, this article uses those writings that profess the use of information as a weapon rather than those that boast the effective use of information in warfare in supporting combat operations, since the latter is not relevant to the question of whether information is a weapon.

The Information Weapon

Identifying literature that advocates information as a weapon is fairly elementary. The authors usually declare their beliefs with such definitive statements as “The electron is the ultimate precision guided weapon”;8 “Information is both the target and the weapon”;9 “The day may well come when more soldiers carry computers than carry guns”;10 “The US may soon wage war by mouse, keyboard and computer virus”;11 “Information may be the most fearsome weapon on the emerging techno-battlefield”;12 “The most potent new US weapon, however, is not a bomb, but a ganglion of electronic ones and zeroes”;13 and “In Information Warfare, Information Age weaponry will replace bombs and bullets.”14 Certainly this is not a comprehensive list of information warfare–related writings that proclaim information as a weapon, but it does represent a cross section of ideas that appear in publications that range from official government documents to more popular books and magazines meant to attract the average reader.

After one gets past the attention-getting steps of pithy statements proclaiming information as a weapon and a target, one significant theme emerges. Specifically, the "information weapon" advocates believe "information warfare can enhance power projection by diminishing an adversary's will and capacity to make war."15 Linking the information weapon to the enemy's war-fighting capabilities and will to fight is significant because US military thinking has evolved to accept that diminishing these two aspects of an opponent will lead to victory for our own forces.16 The US Army field manual on information warfare explains the significance of this linkage by equating the information weapon to the purpose of firepower in combat—"the generation of destructive force against an enemy's capabilities and will to fight."17

Similarly, literature not under the purview of the Department of Defense (DOD) also expounds on the ability of the information weapon to affect the enemy's ability and will to fight. The most apparent difference between official DOD publications and popular literature is that the latter may not employ the exact phrase of using information to affect "the adversary's will and capacity to make war." Nevertheless, this is a firmly established concept that appears frequently in writings about information warfare. For example, Col Richard Szafranski, USAF, Retired, a former Air War College professor who has written extensively on various military-related topics, equates subduing the enemy's will to "neocortical warfare," which "strives to influence, even to the point of regulating the consciousness, perceptions, and will of the adversary's leadership: the enemy's neocortical system."18

Other advocates of the information weapon either do not specifically address what constitutes a “target” or tend to agree in principle with the Air Force definition. While the latter group of advocates agrees that the target is information, their description of the “information target” may be more esoteric. As a case in point, Stein explains that “information attack, while ‘platform-based’ in the physical universe of matter and energy, is not the only counter-platform,” and he believes that doctrinal thinking must move away from the “idea that information attack involves only the use of computers and communications.”19 He incorporates John Boyd’s “observation-orientation-decide-act” (OODA) loop20 in defining the targets of the information weapon. Stein sees indirect information warfare attacks as affecting the “observation” level of the OODA loop at which information must be perceived to be acted on.21 On the other hand, direct information warfare corrupts the “orientation” level of the OODA loop to affect adversary analysis that ultimately results in decision and action.22 Thus, to him, the information weapon may or may not be used against a counterplatform. Stein’s bottom line is that “information is both the target and the weapon: the weapon effect is predictable error.”23 The weapons effect of “predictable error” resulting from the use of the information weapon is an incredible notion because it assumes that one can predictably induce errors an adversary will make in “observing” and “orienting” information that ultimately results in decision and action.

In another example, Szafranski, in the most general terms, appears to agree that the information weapon affects the information target but wants his readers to focus on the “enemy mind” as a whole. He states that the target system of information warfare can include every element in the epistemology of an adversary. *Epistemology* means the entire “organization, structure methods, and validity of knowledge.” In layperson’s terms, it means everything a human organism—an individual or a group—holds to be true or real, no matter whether that which is held as true or real was acquired as knowledge or as a belief.24

In Szafranski's construct, the "acme of skill" is to employ the information weapon to "cause the enemy to choose not to fight by exercising reflexive influence, almost parasympathetic control, over products of the adversary's neocortex."25

Thus, the prototypical advocate of using information as weapons espouses the aim of such weapons as to influence an adversary's will and capacity to make war. Further, with information as the weapon, its target, in the simplest sense, is also information. A more esoteric definition of the target is the enemy mind or his cognitive and technical abilities to use information. Finally, the explicitly stated and sometimes implicitly assumed weapons effect is predictable error. Specifically, the use of the information weapon will allow one to predict how an enemy will err in judgment, decisions, and actions.

Enemy Will and Capacity to Fight

There is a paucity of evidence available for analysis in addressing the information weapon's effect on the "adversary's will and capacity to fight." Most of the literature tends to identify either "information" or the "enemy mind's ability to observe and orient" as the targets of the information weapon. Unfortunately, these two concepts can either encompass every target or are so esoteric that it is difficult to identify specific targets. The remainder of this portion of the analysis will first address the "information" target and then tackle the target of the "enemy mind's ability to observe and orient."

It appears that the US Air Force has recognized the difficulty of identifying specific information targets and has attempted to address the issue through its *Cornerstones of Information Warfare* pamphlet and draft doctrinal documents. For example, the Air Force has stated, “Information warfare is any attack against an information function, regardless of the means.”26 Therefore, “bombing a telephone switching facility is information warfare. So is destroying the switching facility’s software.”27 Similar types of targets may then include elements of the enemy integrated air defense system (IADS). In defining the information target, the US Air Force is attempting to focus information warfare as “a means, not an end, in precisely the same manner that air warfare is a means, not an end.”28 However, an unintended consequence may result from this overarching target definition: if information warfare encompasses nearly every target, then the concept merely becomes a new label for traditional military operations (such as psychological operations, deception, physical destruction, etc.) that military forces have conducted for thousands of years.

Do the information weapon attacks against communications and control facilities, the enemy’s IADS, and their computers diminish the adversary’s will and capacity to fight? Well, yes and no. Certainly, “hard killing” elements of the enemy information functions or “soft killing” through introduction of viruses and logic bombs into the enemy’s computer systems would affect his capacity to fight. Hard kills result in the physical destruction of information systems and interconnections, while soft kills render computer screens “blank” or cause the systems to present faulty displays.

Given that the information weapon could affect an enemy’s capability to fight, will it also be able to affect his will to fight? While the enemy computer terminal operator may feel frustrations and even decreased morale resulting from leaders’ demands for unavailable information, the latter’s will to fight may or may not be affected. In other words, how would “blinding” enemy leaders affect their will to fight? Would they actually surrender, or would US blinding operations actually backfire and force adversary leaders to panic and resort to the use of weapons of mass destruction? For example, Russia adopted a military doctrine in November 1993 that indicated a belief that during an East-West conflict, an attack on Russia's early-warning system for strategic nuclear forces is possible.29 In such a situation, the Russians may assume the worst—the invasion of Russian territory by foreign military forces. With their sensors blinded and command and control systems destroyed by information weapons, Russian leaders may not be able to obtain information and may resort to whatever means necessary to protect their homeland. In essence, they will be "blind," but their strategic nuclear weapons will still be intact and operable. How can the information weapon advocate be certain that Russia will not employ the nuclear weapons?

Instead of just contemplating whether the information weapon will affect an enemy's will to fight, one should ask how US military leaders would react if an adversary blinded friendly command and control systems. Would US military leaders lose the will to fight if their computers went blank? The will to fight is an elusive target, and it is difficult to assess whether the information weapon is capable of affecting it. Certainly, other factors such as political objectives and the question of whether the enemy is fighting for his own survival or for more limited goals would surely figure into the will-to-fight equation.

Despite the value of "will," some information weapon advocates, drawing from Col John Warden's view of the enemy as a system, argue that the relationship of will (morale) and the capacity to fight (physical) can be expressed in the following equation:30

$$(\text{Physical}) \times (\text{Morale}) = \text{Outcome}$$

Specifically, they believe that a weapon need not affect both will and capacity to fight to put the enemy in such a condition that he can no longer carry on the fight. In fact, Colonel Warden states that the physical part of the equation is easier to target than morale, so US forces should focus on the physical. He asserts, "If the physical side of the equation can be driven close to zero, the best morale in the world is not going to produce a high number on the outcome side of the equation."31 Clausewitz cautioned against this type of reductionism and wrote, "If the theory of war did no more than remind us of these elements, demonstrating the need to reckon with and give full value to moral qualities, it would expand its horizon, and simply by establishing this point of view would condemn in advance anyone who sought to base an analysis on material factors alone."32

Indeed, numerous historical cases support Clausewitz's warning of not underestimating the importance of morale or the will to fight. One of the most distinct examples for the United States remains the Vietnam War during the 1960s and early 1970s. Despite the US military's efforts in destroying the Vietnamese communists' material resources and significantly reducing the movement of their lines of communication along the Ho Chi Minh Trail, the communists retained their will to fight.33 In the end, it was their tremendous will to fight and, arguably, the US lack of will to fight that allowed North Vietnam to defeat the United States and the Saigon regime.34

Nevertheless, advocates of the information weapon's effectiveness use the "information warfare" actions in Operation Desert Storm to show that destruction of the capacity to fight (physical) affected the will to fight (morale):

Coalition forces spent the early days of Desert Storm gouging out the eyes of Iraq, knocking out telephone exchanges, microwave relay towers, fiber optic nodes and bridges carrying coaxial communications cables. By striking Hussein's military command centers, the coalition severed communications between Iraqi military leaders and their troops. With their picture of the battlefield—their battlefield awareness—shrouded in a fog, the Iraqis were paralyzed.35

Noticeably lacking from this illustration is the explanation that after the supposed "paralysis" of the Iraqis, deployed coalition military forces fought an air and ground war in Iraq. The combination of coalition air forces that bombed Iraqi targets from 17 January to 2 March 1991 coupled with the coalition ground attack that began on 24 February 199136 ultimately led to Iraq's agreement to accept all terms of the United Nations cease-fire resolution.37 In other words, the efforts to blind and paralyze the Iraqis, while impressive and important, did not by themselves diminish their capability or will to fight. Rather, the blinding efforts made the Iraqis more vulnerable to conventional coalition military attacks and operations.

The Operation Desert Storm illustration, besides being a reductionist argument that distorted the nature and causes of US and coalition military successes against the Iraqi forces, also ignored other realities. First, several Desert Storm analysts suspected that after coalition forces destroyed Saddam Hussein's more advanced telecommunications systems (satellite, microwave, and cable systems), he continued to relay launch orders to his Scud missile batteries via courier.38 Second, the often simplistic method depicted regarding the ease with which the United States took down the Iraqi command network may have been overstated.39 Specifically, while coalition airpower greatly reduced the capacity of the communication links between Baghdad and its field army in the Kuwaiti theater of operations, sufficient connectivity remained for Baghdad to order a withdrawal from Kuwait that included some redeployments to screen the retreat. Therefore, the ambitious hope that bombing the leadership and command, control, and communications targets would lead to the overthrow of the Iraqi regime and completely sever communications between the Baghdad leadership and their military forces “clearly fell short.”40 Third, the Iraqi forces, the Republican Guards notwithstanding, were poorly trained and motivated, and lacked high morale prior to any coalition information attack. Thus, it was not the effect of the information weapon alone that weakened the enemy’s will to fight.

There are other examples of military forces that continued to fight after being isolated from higher headquarters when their communications became inoperable. During the Normandy campaign in 1944, German forces often fought under emissions control or radio silence. Yet, their effective training, sound tactical leadership and doctrine, and adherence to *Auftragstaktik*, or mission-type orders, enabled them, for almost two months, to fight the numerically superior Allies to a stalemate before attrition finally wore down their effectiveness.41

Perhaps those who advocate using the information weapon against the second type of information target, the “enemy mind’s ability to observe and orient,” place more importance on the morale factor than the physical. Champions of attacking this type of information target have coined this form of information warfare as “perception management,”42 “orientation management,”43 or “neocortical warfare.”44 While these terms may imply some “new” types of warfare, in actuality they are merely amorphous terms for what had been traditionally called psychological operations, propaganda, and military deception. For the purpose of discussion, this article addresses this form of information weapon as perception management.

The same question posed about information as a target also applies to the second information target, the enemy mind. The key question is whether information warfare will necessarily reduce the mental ability and will to resist. While it is true that perception management can deceive, surprise, add to the enemy’s fog and friction, and even affect the morale or the will to fight, it will not likely produce a “predictable error” as Dr. Stein assumes.45 The concept of producing a “predictable error” implies that one can predictably induce advantageous errors in an adversary’s actions and decision making. In essence, it assumes that human behavior and reactions are totally predictable and may be precisely manipulated. This concept ignores Clausewitz’s philosophy of the unpredictability of humans and warfare as illustrated through the following syllogism:

If A [does not equal] B (If humans do not behave according to laws)

And C = A (And warfare is a human event)

Therefore, C [does not equal] B (Therefore, warfare will not follow laws)

Not only does the concept of “predictable error” ignore Clausewitz’s theory regarding human nature and warfare, it also seems to challenge common sense. For example, is it really possible to predict the actions, intent, and decision-making rationale of such disparate minds as those of Adolf Hitler, Joseph Stalin, Ho Chi Minh, Ayatollah Ruhollah Khomeini, Mu‘ammar Gadhafi, Saddam Hussein, Mohammed Aidid, and Kim Jong Il? Hitler thought he could achieve a predictable outcome when he drew up the Operation Barbarossa plan and “believed nothing less than the Soviet Union could be defeated in four months.”46 Yet, in April 1945, Soviet tanks entered Berlin, almost four years after German forces invaded the Soviet Union in May 1941. A “predictable error” may be extremely difficult to predict, much less to induce.

In the same vein, perception management will likely have minimal impact on the enemy’s capacity to fight, unless, of course, the “information attack” deceives the enemy regarding the disposition and location of friendly forces. As an illustration, the World War II Allied deception plan, Operation Fortitude, contributed to Adolf Hitler’s preconceptions of the location of the impending invasion of France. Consequently, invading Allied forces at Normandy did not face the bulk of the German troops in France and Belgium guarding the Pas de Calais and the Belgian and Dutch coastline.47

Somewhat more troublesome is the view of many of these advocates who believe it is possible to use the perception management weapon to target the enemy mind with “the aim of subduing hostile will without fighting.”48 They balk at the view that this type of attack should supplement and enhance more conventional forms of warfare. Again, the literature is sparse in terms of specifics on how perception management will “subdue hostile will.” But it does not lack in promises to stop a war before it starts. One example of how this type of attack might target hostile will was posed by Thomas Czerwinski, a professor in the School of Information Warfare and Strategy at the National Defense University. “What would happen if you took Saddam Hussein’s image, altered it, and projected it back to Iraq showing him voicing doubts about his own Baath Party?” While it is not possible to state with absolute certainty the reactions of the Baath Party, Saddam Hussein, or the world community, it is unlikely that such perception management attacks will completely subdue hostile enemy will. Those who predict it is possible to subdue enemy will with perception management seem to assume, as in this example, that enemy leaders will have no interactions with their followers.

Civilian and military leaders have used perception management, or propaganda, throughout the history of warfare. The difference today is brought about by the advent of the microprocessor, which allows another medium, cyberspace, for friendly forces to propagate the perception management message to the enemy.

Unfortunately, propaganda has had, at best, limited utility. To elevate its stature above that of a supplemental role in war is unrealistic.

It is inconceivable to expect perception management alone to subdue a hostile's will to fight, especially when history has shown otherwise. The idea that perception management will enshroud the enemy in "fog" and "friction" and subsequently subdue his morale assumes the enemy will react exactly as the propaganda plan expects. This assumption discounts historical cases. For example, during World War II, the US military, having nearly destroyed Japan's capacity to fight, targeted the will of the people through leaflet drops and firebombings of cities with populations over one hundred thousand, along with the release of two atomic weapons on Hiroshima and Nagasaki. Despite the horrific death and destruction, Japanese military commanders refused to surrender, and the Japanese people were in despair after hearing of their emperor's decree to surrender.49 How realistic, then, is the information weapon advocates' vision that enemies will surrender through information attacks targeted at the enemy mind or "neocortical" system? Will the enemy stop fighting because the United States, through perception management attacks, tells him to stop? Unfortunately, the enemy may not always be so cooperative.

The Information Weapon: Use with Caution

In analyzing whether information is a weapon, this article tested the ability of information itself to target "information" and the "enemy mind's ability to observe and orient" for the purpose of destroying the enemy's will and capacity to fight. The results indicated that while information may be considered a weapon, it is one that must be used with caution. The more enthusiastic proponents of the information weapon tend to overestimate its ability to diminish enemy capacity and will to fight.

Information is not a technological “silver bullet,” able to subdue the enemy without battle. Unlike other, more conventional, weapons, the effects of the information weapon are not necessarily predictable because it often targets the human mind and emotions. Thus, in employing the information weapon, one must not rely solely on its use for success. Rather, the strategist must prudently use the information weapon to supplement more traditional weapons of war or as a precursor to conventional attacks and operations.

While this article has answered the question it set out to investigate, other factors have emerged in the course of this analysis. The extreme claims for information warfare, even when employing the information weapon as envisioned by its advocates, are particularly unconvincing and even irresponsible. The most zealous advocates of information warfare describe information as a low-cost weapon with a high payoff, a method to eliminate the fog and friction of war for friendly forces yet enshroud the enemy in the same, and a tool to allow attainment of quick and bloodless victories.

Regarding the first characteristic, a low-cost weapon with a high payoff, the cost will depend on the specific information weapon itself. Certainly, introducing a virus or logic bomb into a computer system may be a relatively low-cost option, whereas physical destruction of the enemy IADS will likely accrue significant costs. The claim of a high payoff is also debatable. As previously discussed, “predictable errors” may be extremely difficult to predict and induce as the information weapon often targets human reactions and emotions.

In an ideal world, fog and friction would be eliminated for friendly forces and yet maximized against the enemy. However, the exact information weapons intended to increase the enemy’s “fog of uncertainty" may lead to totally unintended consequences that are inconsistent with the original intent of the weapon. Worse, the nth-order effect may actually prove counterproductive to the original intent and objective. In a complex, hierarchical command and control system, destruction of selected communications connectivity may actually result in a more streamlined and efficient command and control system. At least three unintended consequences may result. First, the enemy leader, without the intermediate command and control steps, is now able to send his orders directly to the lower echelons. For example, during Operation Desert Storm, after coalition forces destroyed Saddam Hussein's more advanced telecommunications capabilities, he continued to relay launch orders to his Scud missile batteries via courier.50 Second, if communications connectivity is severed, lower echelons will likely operate in autonomous modes. While they may lack the complete situational battlefield picture that upper echelons would normally provide, the lower echelons benefit by not having to wait for launch orders to flow from the top. Third, destroying or degrading enemy command and control systems may deny friendly forces the ability to collect vital enemy communications and signals. Thus, employment of the information weapon may actually simplify enemy operations and increase friendly fog and friction, since friendly collection assets will not be able to collect against emitting enemy electronic systems.

Perhaps the most disturbing claim is that of the information weapon's capability to attain quick and bloodless victories and its extreme view of preventing a war before it starts. While the information weapon may be able to prevent bloodshed in a limited number of scenarios, expecting it to end a war before the first shot is fired is pure speculation. A more realistic consequence resulting from the employment of the information weapon would be a degraded enemy that lacks complete battlefield situational awareness because leaders are blinded and cannot communicate with troops in the field. There is a lack of historical evidence that supports the concept that a blinded enemy would simply surrender without fighting. On the contrary, history shows military forces, isolated from higher headquarters, do continue to fight. As previously mentioned, the German military, during World War II, emphasized *Auftragstaktik*, which relied on general guidance from above combined with lower echelon initiative.51 This philosophy resulted in German forces fighting under radio silence, without upper echelon guidance, as during the Allied Normandy campaign.

Maj Gen Michael V. Hayden, commander of the Air Intelligence Agency, summed it best when he called the “notion of a bloodless war played out on computers as fanciful” and said that he does not foresee the United States mothballing its stockpile of conventional and nuclear weapons in the near future. Further, he stated, “Can I imagine a time in which we won’t have destructive war? No. But I think it’s easy to imagine a time when we can use information as an alternative to traditional warfare.” General Hayden relayed the following incident to describe the use of the information weapon to help create the zone of separation between warring factions in Bosnia:

Some of the factions didn’t comply completely. But the Implementation Force goaded, forced, cajoled and pressured them to do it. One of the things they did was take clear evidence [and] information that they had not complied with the treaty. The IFOR commander turned to the Serb, the Croat and the Muslim and said, “Move those tanks.” Their response was “What tanks?” The commander says, “These tanks,” pointing to the concrete evidence. “Oh, those tanks,” they said. And then the tanks were moved. In Bosnia, I think it’s fair to say, information is the weapon of first resort. To back that up is the potential for heat, blast and fragmentation. But in this case, information was used as an alternative. We achieved an objective without going immediately to some sort of destructive approach.52

It is clear that while information may be used as a weapon, strategists must use it with caution and common sense. It is not a silver-bullet weapon. Rather, the strategist should plan the use of the information weapon in conjunction with more traditional weapons and employ it as a precursor weapon to blind the enemy prior to conventional attacks and operations.

The US military arsenal includes a variety of weapons, and the strategist must ensure their most effective use in future wars. The strategy of the future will likely include the use of the information weapon in conjunction with more conventional weapons. In developing the plan, the strategist must realize that the use of the information weapon will demand prudence and carry implications that may impact the employment of the weapon. The last section warns of the additional cautions that a strategist planning to employ the information weapon must consider.

Implications

One characteristic of the US military and its way of war is its fascination with technology and the associated search for the high-tech silver bullet that will allow quick victories with minimal collateral damage.53 Hence, it is not surprising that extremists have embraced information warfare as the magic weapon that would allow the US military to win bloodless victories and end wars before the first bullet is ever fired. The use of the information weapon demands caution, and its employment carries with it implications that the strategists must consider.

First, perhaps one reason for the vast interest in the application of information warfare is that the United States may be the most vulnerable to its effects. As Lt Gen Kenneth A. Minihan, director of the National Security Agency, explained, “Information is both the greatest advantage and, given American dependency on information, the greatest weakness of the US.”54 Consider the following assertion: “Under IW, the enemy soldier no longer constitutes a major target. IW will focus on preventing the enemy soldier from talking to his commander. Without coordinated action, an enemy force becomes an unwieldy mob, and a battle devolves to a crowd-control issue.”55 Is this actually an analysis of the vulnerability of our own US military to information warfare? Given the US system of assigning specific targets to individual aircraft via the air tasking order (ATO), the descriptions of enemy vulnerability to the information weapon may actually be a reflection on the American air campaign process. Could an information weapon bring the air operations center (AOC) to a standstill if it destroyed computers within the AOC, leaving it with no capability to develop and transmit the ATO to flying wings?

A second implication concerns the importance of maintaining US combat readiness with conventional military forces. Eliot Cohen, noted author and professor at Johns Hopkins University, warned, “Transformation in one area of military affairs does not, however, mean the irrelevance of all others. Just as nuclear weapons did not render conventional power obsolete, this revolution will not render guerrilla tactics, terrorism, or WMD [weapons of mass destruction] obsolete.”56 The US military must, therefore, remain capable of fighting less technologically advanced enemies as well as peer competitors. History is full of examples of less technically developed militaries overcoming and defeating more “capable” foes. The most vivid example for the United States remains the Vietcong, who were able to defeat technology with rudimentary tactics and a willingness to sacrifice their soldiers. In facing a Vietcong-type adversary, can the United States realistically expect to defeat an enemy without resort to heavy destruction, or at least having in place the potential to do such destruction?57

A third implication that civilian and military leaders must seriously consider is the legality of information warfare. This question is especially important when one considers “preemptive” information attacks. One envisioned characteristic of information warfare regards the use of the information weapon to end a war before the first shot is fired. How will the international community react to this type of preemptive attack by the United States, a superpower, especially if it is against a third world rogue power? Is the United States willing to risk an information attack that would blind a peer competitor and risk escalating the conflict with the use of weapons of mass destruction? Is an information attack an act of war? Further, the use of perception management, especially one that alters an enemy leader’s image to tell his people to surrender, is comparable to faking surrender with the use of the traditional white flag. This and other actions may violate the “principle of chivalry which addresses the use of trickery,” both permissible ruses and impermissible perfidy and treachery.”58

Obviously, the potential consequences of the employment of the information weapon are new and evolving, and the implications of information warfare raise many issues that have no clear legal precedent.59

Conclusion

The information weapon may be an effective tool to supplement the military’s arsenal of more traditional weapons. Further, its use as a precursor may enhance conventional attacks and operations against a blinded and degraded enemy, thus decreasing effective enemy defense and counterattacks. However, the United States should not consider the information weapon a “silver bullet” that will completely subdue an adversary’s will and capacity to fight.

Further, strategists must refrain from uncritically assuming the information weapon is capable of terminating wars before the first bullet is even fired.

The US civilian and military leaders should strive to understand why information warfare appears so attractive, in order that realistic and useful doctrinal guidance may be developed for its employment and incorporation into the overall war-fighting strategy. The consequences of not accomplishing this self-examination could result in the military promising too much, too fast.

Notes

1. Dr. George J. Stein, director, International Security Studies core and professor of European Studies at the US Air Force Air War College, Maxwell AFB, Ala., interviewed by author, 9 October 1996. Dr. Stein’s interest in information warfare began with his participation in the Air Force chief of staff–directed SPACECAST 2020 study at Air University, Maxwell AFB, Ala., in academic year 1994/1995.

2. Dr. George J. Stein, “Information Attack: Information Warfare in 2025,” in *2025 White Papers: Power and Influence,* vol. 3, bk. 1 (Maxwell AFB, Ala.: Air University Press, November 1996), 98. [See also, Stein's "Information Warfare," *Airpower Journal*, Spring 1995.]

3. USAF, *Cornerstones of Information Warfare* (Washington, D.C.: Department of the Air Force, 1995), 2.

4. Ibid.

5. Soon after Operation Desert Storm, several noted authors claimed that Operation Desert Storm was the “first information war.” They include Alan D. Campen, ed., *The First Information War* (Fairfax, Va.: AFCEA International Press, October 1992); and

Alvin Toffler and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (New York: Little, Brown & Co., 1993).

6. Campen, vii. Other examples include Toffler and Toffler, 69. The Tofflers stated that the Gulf War represented a completely "new form of warfare." They asserted that "a revolution is occurring that places knowledge, in various forms, at the core of military power." Three RAND defense analysts asserted that "Desert Storm represented the first modern 'information war,' in that every aspect of military operations depended to some degree on information provided by many systems operating in various media and at all echelons." James A. Winnefeld, Preston Niblack, and Dana J. Johnson, *A League of Airmen: US Airpower in the Gulf War* (Santa Monica, Calif.: RAND, 1994), 182 and 219.

7. Col Edward C. Mann III, *Thunder and Lightning: Desert Storm and the Airpower Debates* (Maxwell AFB, Ala.: Air University Press, April 1995), 146. Colonel Mann directly challenged Alan Campen's claim that Operation Desert Storm was the "first information war" by pointing out that "Campen tacitly avers the truth—suggested by Sun Tzu 2,500 years ago—that the ultimate goal of the struggle is to dominate the enemy in knowledge—not information. Collection and analysis of information is, of course, a part—but not the whole—of the issue."

8. Quoted in John T. Correll, "Warfare in the Information Age" (editorial), *Air Force Magazine* 79, no. 12 (December 1996): 3. John M. Deutch, former director of Central Intelligence (DCI), testified on 25 June 1996 before the US Senate Committee on Government Affairs on the subject of "Foreign Information Warfare Programs and Capabilities." Deutch had served dual-hatted roles as both the DCI and director, Central Intelligence Agency (CIA). The National Security Act of 1947 designates the DCI as the primary adviser on national foreign intelligence to the president and the National

Security Council. The DCI is tasked with directing and conducting all national foreign intelligence and counterintelligence activities. To discharge these duties, the DCI serves both as head of the CIA and of the US Intelligence community. It was in his DCI capacity that Deutch testified before the US Senate. In discussions regarding offensive information warfare capabilities, Deutch told Congress that "the electron is the ultimate precision guided weapon." His opening remarks during this testimony are on-line, Internet, 17 March 1997, available from http://www.odci.gov/cia/public_affairs/speeches/dci_testimony_062596.html.

9. *Cornerstones of Information Warfare*, 2–3; and Stein, "Information Attack," 105.

10. Toffler and Toffler, 71.

11. Douglas Waller Washington, "Onward Cyber Soldiers," *Time*, 21 August 1995, n.p.; on-line, Internet, 26 January 1997, available from http://pathfinder.com/@@LL1c6QYAspdOHaCM/time/magazine/domestic/1995/950821.cover.html.

12. Peter Grier, "Information Warfare," *Air Force Magazine* 78, no. 3 (March 1995): 34.

13. Richard J. Newman, "Warfare 2020," *U.S. News and World Report* 121, no. 5 (5 August 1996): 35.

14. Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (New York: Thunder's Mouth Press, 1994), 15.

15. US Air Force Doctrine Document (AFDD) 1, "Air Force Basic Doctrine," 21 May 1996 (second draft), 9.

16. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976), 90.

The concept of defeating an adversary's will and capacity to make war may be traced to the writings of Carl von Clausewitz as he defined three broad objectives of war "which between them cover everything: the *armed forces*, the *country*, and the *enemy's will*." This concept has permeated US military thinking as demonstrated by its inclusion in military doctrine, including Joint Pub 3-0, *Doctrine for Joint Operations,* 1 February 1995; US Army Field Manual (FM) 100-5, *Operations,* June 1993; Air Force Manual (AFM) 1-1, *Basic Aerospace Doctrine of the United States Air Force*, vol. 1, March 1992; and AFDD 1.

17. FM 100-6, *Information Operations*, August 1996, 1–12.

18. Col Richard Szafranski, "Neocortical Warfare? The Acme of Skill," *Military Review*, November 1994, 42.

19. Stein, "Information Attack," 114.

20. John R. Boyd, "A Discourse on Winning and Losing," briefing slides, Air War College, Maxwell AFB, Ala., August 1987. Boyd's "observation-orientation-decide-act" (OODA) loop is based on the concept that "every individual operates an OODA loop that is unique in speed and accuracy. Speed is based on the individual's mental capacity and capability to deal with information and changing environments. John Boyd asserts that one can paralyze an enemy by operating inside the opponent's OODA loop, meaning that the individual is operating a faster cycle speed than the enemy's. Accuracy is determined during the orient part of the cycle by what information is filtered and how it is organized. Boyd considers the orientation as the most important part of the cycle because 'it shapes the way we interact with the environment—hence orientation shapes the way we observe, the way we decide, the way we act.' " This description of Boyd's OODA loop is taken from "Information Operations: A New War-fighting Capability," Lt

Col William Osborne et al., in *2025 White Papers: Power and Influence,* vol. 3, bk. 1, 49.

21. Stein, "Information Attack," 114. Stein explained that "in many cases, indirect IW will be platform-to-platform as, for example, offensive and defensive electronic warfare, jamming or other interference systems, and psychological operations via the successor systems to *Commando Solo*. It may, however, rely on nonelectronic old-fashioned military deception and psychological operations."

22. Ibid. Stein described corruption of the "orientation" portion of the OODA loop: "adversary analysis, whether artificial-intelligence or information-technology based or, most importantly, based in the mind of the human decision maker, decides and acts with full confidence in either the information observed or the integrity of his (machine or human) analytic processes."

23. Ibid.

24. Col Richard Szafranski, "A Theory of Information Warfare: Preparing for 2020," *Airpower Journal* 9, no. 1 (Spring 1995): 60.

25. Ibid., 44.

26. *Cornerstones of Information Warfare*, 4.

27. Ibid.

28. Ibid.

29. Sumner Benson, "How New the New Russia? Deep-Strike Weapons and Strategic Stability," *Orbis*, Fall 1996, 509.

30. Col John A. Warden III, "The Enemy as a System," *Airpower Journal* 9, no. 1 (Spring 1995): 43.

31. Ibid.

32. Clausewitz, 184.

33. Eduard Mark, *Aerial Interdiction: Air Power and the Land Battle in Three American Wars* (Washington, D.C.: Center for Air Force History, 1994), 363. Mark explains that "the greatest single advantage of the Communists in resisting interdiction, other than their low logistical requirements, was that they were usually free to give battle or to decline it at will."

34. Earl H. Tilford Jr., "The Prolongation of the United States in Vietnam," in *Prolonged Wars: A Post-Nuclear Challenge*, ed. Dr. Karl P. Magyar and Dr. Constantine P. Danopoulos (Maxwell AFB, Ala.: Air University Press, 1994), 371 and 389. Tilford proclaims that "Hanoi won the Vietnam War." He explains that North Vietnam and the Vietcong forces sustained their will to fight. "For the communists, their fight with the United States and the Saigon regime was purposeful. Their objectives were constant, achievable, and better defined. Their political and military leaders, in working to achieve those objectives, devised superior strategies which, eventually, produced victory. The communists wanted to make the Americans suffer—over an extended period of time—until they gave up."

35. TSgt Pat McKenna, "Info Warriors: Battling for Data Dominance in the Fifth Dimension," *Airman Magazine*, September 1996, n.p.; on-line, Internet, 22 January 1997, available from http://www.af.mil/pa/airman/0996/info.htm.

36. Thomas A. Keaney and Eliot A. Cohen, *Revolution in Warfare? Air Power in the Persian Gulf* (Annapolis, Md.: Naval Institute Press, 1995), 236–37.

37. James P. Coyne, *Airpower in the Gulf* (Arlington, Va.: Aerospace Education Foundation, 1992), 190.

38. Michael R. Gordon and Gen Bernard E. Trainor, *The Generals' War: The Inside Story of the Conflict in the Gulf* (Boston, Mass.: Little, Brown and Co., 1995), 246–48; and Steven K. Black, "Information Warfare in the Post–Cold War World" (paper submitted as part of the Air Force Fellow Program to the Matthew B. Ridgway Center for International Security Studies, University of Pittsburgh, 1996), 16.

39. John R. Levine and Carol Baroudi, *The Internet for Dummies*, 2d ed. (San Mateo, Calif.: IDG Books Worldwide, Inc., 1994), 12. The authors ask, "Can the Internet really resist enemy attack?" and answer, "It looks that way. During the Gulf War in 1991, the US military had considerable trouble knocking out the Iraqi command network. It turned out that the Iraqis were using commercially available network routers with standard Internet routing and recovery technology. In other words, dynamic rerouting really worked. It's nice to know that dynamic rerouting works, although perhaps this was not the most opportune way to find out."

40. Keaney and Cohen, 60.

41. Col Trevor N. Depuy, *A Genius for War* (Fairfax, Va.: Hero Books, 1984), 4. Also R. L. DiNardo and Daniel J. Hughes, "Some Cautionary Thoughts on Information Warfare," *Airpower Journal* 9, no. 4 (Winter 1995): 76.

42. Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, Calif.: RAND, 1996), 22–23. Perception management is "manipulating information that is key to perceptions."

43. Stein, "Information Attack," 91, 114. Dr. Stein states, "Information attack is not so much perception management as orientation management. Information is both the target and the weapon; the weapon effect is predictable error."

44. Szafranski, 45.

45. Stein, “Information Attack,” 91, 114.

46. Richard Overy, *Why the Allies Won* (New York: W. W. Norton & Co., 1995), 13.

47. Ibid., 151.

48. Szafranski, 42.

49. Thomas B. Allen and Norman Polmar, *Code-Name Downfall: The Secret Plan to Invade Japan and Why Truman Dropped the Bomb* (New York: Simon & Schuster, 1995), 258–89.

50. Gordon and Trainor, 246–48. Also, Black, 16.

51. Depuy, 4. Also DiNardo and Hughes, 76.

52. McKenna, n.p.

53. Several noted authors have warned of this phenomenon regarding the US fascination with technology and with finding a silver-bullet weapon that allows quick victory with minimum collateral damage. They include Earl H. Tilford Jr., *The Revolution in Military Affairs: Prospects and Cautions,* report (Carlisle Barracks, Pa.: Strategic Studies Institute, US Army War College, 23 June 1995), 4; Charles J. Dunlap, “How We Lost the High-Tech War of 2007: A Warning from the Future,” *The Weekly Standard* 1, no. 19 (29 January 1996): passim; DiNardo and Hughes, 69; and Black, 1.

54. John A. Tirpak, “Shifting Patterns of Air Warfare,” *Air Force Magazine* 80, no. 4 (April 1997): 26.

55. Capt George A. Crawford, “Information Warfare: New Roles for Information Systems in Military Operations,” *Air Chronicles:* n.p.; on-line, Internet, 26 January 1997, available from http://www.cdsar.af.mil/cc/crawford.html.

56. Eliot A. Cohen, “Revolution in Warfare,” *Foreign Affairs* 75, no. 2 (March/April 1996): 51. Cohen is professor of strategic studies at the Paul H. Nitze School of Advanced International Studies, Johns Hopkins University.

57. Frank C. Mahncke, “Information Warriors*,” Naval War College Review* 47, no. 3 (Summer 1994): 133. This piece appeared as a book review of the Tofflers’ *War and Anti-War: Survival at the Dawn of the 21st Century.*

58. Richard W. Aldrich, “The International Legal Implications of Information Warfare,” INSS Occasional Paper 9 (US Air Force Academy, Colo.: Institute for National Security Studies, April 1996), 1 and 16.

59. Ibid., vii.

Published:

https://cryptome.org/jya/af-infoweap.htm

Review questions:

1. *Do you agree with the statement that information is a weapon?*
2. *Suggest your definition of "information warfare".*
3. *What can be considered an information weapon?*

D. Snetselaar, G. Frerks, L. Gould, S. Rietjens, T. Sweijs

Knowledge security: insights for NATO

Knowledge security entails mitigating the risks of espionage, unwanted knowledge transfers, intellectual property theft, data leakage and the misuse of dual-use technology (technology that is primarily "focused on commercial markets but may also have defence and security applications").

In the context of research on and the development of high-end technology, knowledge security is vital to NATO's ability to deter and defend against adversaries and protect the prosperity of its members. Countering hybrid threats that target critical national security technologies requires a whole-of-society approach that comprises the public sector, private companies, civil society and individuals aligning their principles and standards to engage meaningfully on an issue. The development of such an approach is hindered by diverging threat perceptions, interests and levels of awareness of the stakeholders (civilian and military; private and public) involved. To develop calibrated whole-of-society responses, NATO needs to understand what the opposing imperatives are for different stakeholders and how they can be bridged.

This article examines the contrasting perspectives on a Sino-Dutch research project on Artificial Intelligence (AI) called DREAMS Lab and offers an innovative analytical framework to identify and understand those different perspectives and interests, referred to as the assemblage approach. Assemblage is a concept that has come into usage in international social theory as an alternative to more traditional concepts like 'state', 'alliance' or 'network' to study the emerging and fluid social-material formations in contemporary societies. The assemblage approach is used here to analyse how a group of heterogeneous actors came together and responded to the

DREAMS Lab project despite their different perceptions and, at times, conflicting interests. Similarly, the assemblage approach can help NATO and its Allies recognise and respond to hybrid threats in and beyond the knowledge domain.

Hybrid warfare: the context for knowledge security at NATO

Though ‘hybrid warfare’ is still a contested subject of academic and policy debates, effectively responding to hybrid threats has nonetheless become a top priority for NATO and its members. Opponent states increasingly deploy combinations of hybrid tactics to pursue their strategic interests, often in order to remain below the threshold of armed conflict. As such, hybrid threats are considered a pressing, cross-domain challenge that inhabits a ‘grey zone’ between war and peace. Examples of hybrid threats include disinformation, political meddling, cyber warfare and the theft of technologies.

In the economic domain, hybrid threats pose challenges in relation to energy security, critical infrastructures, foreign direct investments and research on high-end technologies. Such challenges may not have immediate military implications, but are still of vital importance to the resilience of the Alliance and its members. The 2022 Madrid Summit Declaration explicitly mentioned energy security and resilience to cyber and hybrid threats, while Article 2 of the North Atlantic Treaty calls for “economic cooperation” in national security matters such as the abovementioned challenges.

The subject is also pertinent in view of the Artificial Intelligence Strategy for NATO, adopted by Allied Defence Ministers in October 2021, which highlighted the international security risks implied in the field of artificial intelligence. Understanding what knowledge security entails and how it can contribute to achieving resilience against hybrid threats is therefore of particular relevance to NATO.

At issue: Sino-European research collaborations on high-end technology

To illustrate the challenges of responding to hybrid threats in the knowledge domain, we draw on empirical fieldwork conducted in 2021 on a Sino-Dutch research project on AI called DREAMS Lab.DREAMS Lab is a collaborative project run by the University of Amsterdam (UvA) and the Free University of Amsterdam (VU). The project is funded by the Chinese telecommunication company Huawei, which will invest a total of EUR 3.5 million over four years. The aim of the project is to study the use of AI to optimise search engine functionality. Huawei has an interest in optimising its search engine technology as it is banned from using apps like Google Search.

Projects like DREAMS Lab offer several benefits for European research institutions, including access to talent, funding and expertise in key technological areas. Despite these benefits, however, European governments, politicians, think tanks and journalists increasingly perceive collaborations with Chinese research partners as risky in the context of ongoing geopolitical tensions and rivalry.

The development and use of high-end technologies like AI is expected to have a large impact in both economic and military domains. Having access to AI is therefore considered crucial for a country’s economic prosperity and national security. Driven by the ambition to become a world leader in key technological areas including AI, China is often suspected of using international research collaborations to access and acquire the knowledge it needs. Because of this, think tanks warn undesired knowledge transfers, intellectual property theft, data leakage, encroachment on academic freedom and ethical dilemmas (see for example the reports published by the Leiden Asia Centre and the Hague Centre for Strategic Studies).

These concerns have led the Netherlands, but also countries like the United Kingdom, Germany and Sweden, to take preventive measures. Such measures include raising awareness among staff, conducting due diligence, ensuring compliance to dual-use regulations and investing in information security. As will become clear, the DREAMS Lab case offers insights relevant to NATO regarding the nature of hybrid threats in the knowledge domain and could help encourage member countries to take appropriate knowledge security measures.

Case study: the DREAMS LAB project

When a journalist from the Dutch Financial Daily began reporting about the DREAMS Lab project, a fierce debate started to unfold amongst policy makers and academics. The articles questioned the UvA and VU's decision to work with Huawei in light of concerns over state espionage and data theft facilitated by Huawei as a 5G supplier. Though the DREAMS Lab project had nothing to do with 5G, politicians wanted to know why the Dutch government had given approval for the project. The government made clear that the Ministries of Economic Affairs and of Education and the Security Services had only informed the UvA and the VU about the possible risks and that it had not given its formal approval as it has no mandate to do so.

Amongst scholars, the debate focused on the ethics of working with Huawei. The Chinese telecommunication company has been accused of being complicit in the oppression of the Uyghurs (a Muslim ethnic minority living in Xinjiang) by the Chinese government. In October 2020, an assemblage of Dutch scientists and scholars sent an open letter calling on the UvA and the VU to reconsider the project on ethical grounds, as working with Huawei could be construed as symbolically justifying the company’s actions and ethics.

The debate in politics and in academia did not result in the termination of the DREAMS Lab project, but it put ‘knowledge security’ high on the Dutch political agenda. Knowledge security is a term used by the Dutch government (and increasingly by universities) to refer to the risks of working with research partners from countries such as China but also Iran and Russia. After the DREAMS Lab incident, an assemblage of government ministries, universities and national research organisations started working (collaboratively and separately) on practical guidelines to help research institutions assess the security risks and ethical implications of international research collaborations. One of the primary objectives of these knowledge security measures is to ensure a reciprocal exchange of knowledge and expertise and prevent the undesired transfer of sensitive knowledge or technologies.

On 21 July 2021 the resulting Framework Knowledge Security Universities was published by the Association of Dutch Universities (VSNU). The Framework not only encompassed a risk analysis and guidelines, but also offered six concrete instruments to promote knowledge security and prevent abuse, such as a national network of advisory teams, a checklist for international collaboration, a risk and incident register, training sessions and awareness campaigns.

Key insights

Using the assemblage approach, three key insights were drawn from the response to the DREAMS Lab project.

First, the threat representation of DREAMS Lab as both a security and human rights risk helped align the interests of the parties to the assemblage. While the security reading resonated with the government agencies concerned with national security, academics were more concerned with Huawei’s complicity in human rights violations. However, the two threat perceptions were not mutually exclusive, but reinforced one another. Concerns about the implication of undesired knowledge transfer for the Dutch innovation and research community resonated with the Ministries of Economic Affairs and of Education as well as sector organisations like the aforementioned VSNU.

Second, the policy and practice of knowledge security helped to bring the concerns of different actors together and make the threat actionable. Following the debate on DREAMS Lab, the Minister of Education, the State Secretary of Economic Affairs and the Minister of Justice and Security sent a letter to parliament in which they addressed the different risks involved in international research collaborations with countries of concern and explained how these risks pose a threat to knowledge security. The Ministers and State Secretary identified a number of countermeasures, including the development and implementation of the guidelines that resulted in the above mentioned Framework.

Third, the DREAMS Lab project confronted government ministries and universities with questions of responsibility, autonomy, ideological dilemmas and external dependencies. Determining who is responsible for knowledge security and how international research should be regulated not only raised practical issues of capacity and awareness, but also ideological questions on the extent of government involvement while safeguarding academic freedom. In addition, both government and academic institutions were limited in their responses by external dependencies. The competitive position of Dutch scientific research, for example, depends on international collaboration and not least with China, which represents a crucial research partner for the Netherlands outside of Europe (see the following report for the scope of Sino-

Dutch collaboration). Rather than a ban on all collaboration with China, therefore, a tailored and case-by-case approach was favoured by the assemblage.

Responding to cases like DREAMS Lab requires a careful analysis and consideration of the different perceptions, interests and dependencies of the actors involved, and close collaboration across government and society at large. It also inherently entails weighing security interests against economic and scientific interests and against democratic values like academic freedom.

Recommendations

Though we do not argue that NATO should become directly involved in responding to projects like DREAMS Lab, three recommendations for the Alliance flow naturally from this case study.

First, complex challenges like hybrid threats in the knowledge domain, and the economic domain more broadly, require an in-depth understanding of their multi-layered and multi-vectored nature. Specifically, NATO needs to invest more in social science research to understand the nature of the challenge and to formulate effective responses. It does not suffice to recognise these challenges from a purely technical or military-strategic perspective; a broader perspective needs to be adopted. The assemblage approach used to study the DREAMS Lab case can be applied to study similar perceived security threats to help unravel the different actors, technologies, interests and perspectives involved for more tailor-made responses.

Second, based on this research, NATO should invest in raising awareness on how knowledge and technologies can travel across borders and to what effect. In doing so, it should encourage members to take a nuanced and tailored approach and bolster collaboration between military and civilian actors, in and outside governments to address collective challenges. Articles 2 and 3 of NATO's founding treaty create a basis and framework for the Alliance to do so. However, because this requires a whole-of-society approach, NATO needs to understand and consider the perspectives and interests of all stakeholders. In these forms of collaboration, the Alliance can take on the roles of facilitator and enabler of crucial policy and implementation guidelines, while national implementation is the responsibility of individual member countries.

Third and finally, in order to effectively respond to hybrid threats in civilian domains, not just in the knowledge domain, stakeholders must weigh conflicting interests and address inherently political questions. NATO must transparently consider not just security and economic interests, but also the fundamental freedoms that define what the Alliance stands for. For example, such considerations also apply to policies aimed at countering disinformation.

Applying the assemblage approach to the DREAMS Lab case has offered an empirical example of what such a response to hybrid threats in the civilian domain might look like. It has also shown the necessity to deal diligently with the multidimensional dynamics of working with the heterogeneous actors that converge in international academic collaborations.

Published:

https://www.nato.int/docu/review/articles/2022/09/30/knowledge-security-insights-for-nato/index.html

Review questions:

1. *What do you know about Knowledge security?*
2. *What is the potential of using artificial intelligence in the military sphere?*
3. *Why invest in social science research to understand the nature of the challenge and be able to formulate effective responses to it?*

About Jean Monnet

Jean Monnet, (born Nov. 9, 1888, Cognac, France – died March 16, 1979, Houjarray), French political economist and diplomat who initiated comprehensive economic planning in western Europe after World War II. In France he was responsible for the successful plan designed to rebuild and modernize that nation's crumbled economy.

During World War I Monnet was the French representative on the Inter-Allied Maritime Commission, and after the war he was deputy secretary-general of the League of Nations (1919-23). Then, after reorganizing his family's brandy business, he became the European partner of a New York investment bank in 1925.

At the start of World War II he was made chairman of the Franco-British Economic Co-ordination Committee. In June 1940 it was he who suggested a Franco-British union to Winston Churchill. After the Franco-German armistice he left for Washington, D.C., and in 1943 he was sent to Algiers to work with the Free French administration there.

After the liberation of France, Monnet headed a government committee to prepare a comprehensive plan for the reconstruction and modernization of the French economy. On Jan. 11, 1947, the Monnet Plan was adopted by the French government, and Monnet himself was appointed commissioner-general of the National Planning Board. In May 1950 he and Robert Schuman, then the French foreign minister, proposed the establishment of a common

European market for coal and steel by countries willing to delegate their powers over these industries to an independent authority. Six countries – France, West Germany, Italy, Belgium, the Netherlands, and Luxembourg – signed the treaty in 1951 that set up the European Coal and Steel Community (ECSC). From 1952 to 1955 Monnet served as the first president of the ECSC's High Authority. The ECSC inspired the creation of the European Economic Community, or Common Market, in 1957.

In 1955 Monnet organized the Action Committee for the United States of Europe and served as its president from 1956 to 1975. In 1976 the heads of the nine Common Market governments named Monnet a Citizen of Europe. In the same year, he published his Mémoires (Memoirs, 1978).

Source:

Britannica, The Editors of Encyclopaedia. "Jean Monnet". *Encyclopedia Britannica*, 5 Nov. 2022, https://www.britannica.com/biography/Jean-Monnet.

About ERASMUS+ Jean Monnet Actions

Jean Monnet Programme has transformed into Jean Monnet Actions under ERASMUS+ Programme since 2014.

The **Jean Monnet actions** offer opportunities in the field of higher education and in other fields of education and training. The Jean Monnet actions contribute to spread knowledge about the European Union integration matters. The following actions are supported:

- Jean Monnet Actions in the field of higher education
- Jean Monnet Actions in other fields of education and training
- Jean Monnet policy debate (higher education and other fields of education and training)

These actions will be implemented by **the European Education and Culture Executive Agency (EACEA)**.

The Jean Monnet Actions in the field of Higher Education supports teaching and research in the field of European Union studies worldwide.

European Union studies refers to the teaching, learning and research about the European Union, its history, aims, structures, functions and/or its policies.

The Jean Monnet actions also strive to function as a vector of public diplomacy towards third countries, promoting EU values and enhancing the visibility of what the European Union stands for and what it intends to achieve.

The Jean Monnet "Teaching and Research" actions will:

- promote excellence in teaching and research in the field of European Union studies worldwide;
- foster the dialogue between the academic world and society, including local, regional, state and EU level policy-makers, civil servants, civil society actors, representatives of the different levels of education and of the media;
- generate knowledge and insights in support of EU policy-making and strengthen the role of the EU within Europe and in a globalised world;
- reach out to a wider public and spread knowledge about the EU to the wider society (beyond academia and specialised audiences) bringing the EU closer to the public.

The actions also strive to function as a vector for public diplomacy towards third countries not associated to the Programme, promoting EU values and enhancing the visibility of what the European Union actually stands for and what it intends to achieve.

The Jean Monnet "Teaching and Research" must take one of the following forms: Modules, Chairs, Centres of Excellence

- **Modules** are short teaching programmes or courses in the field of European Union studies at offered at a higher education institution. Each Module has a minimum duration of 40 teaching hours per academic year for a duration of three years. Modules may concentrate on one particular discipline in European studies or be multidisciplinary in approach and therefore call upon the academic input of several professors and experts. They can also take the form of short specialised or summer programmes.
- **Chairs** are teaching posts with a specialisation in European Union studies (as described above) for university professors for a duration of three years. A Jean Monnet Chair is held by only one professor, who provides the minimum of 90 teaching hours per academic year. The Chair may also have a team to support and enhance the activities of the Chair, including the provision of additional teaching hours.
- **Jean Monnet Centres of Excellence** are focal points of competence and knowledge on European Union subjects. They should gather the expertise and competences of high-level experts aiming to at develop synergies between the various disciplines and resources in European studies (as described above) as well as at creating joint transnational activities, they also ensure openness to civil society. Jean Monnet Centres of Excellence have a major role in reaching out to students from faculties not normally dealing with European Union issues as well as to policy makers, civil servants, organised civil society and the general public at large.

Sources:

Jean Monnet Actions: https://erasmus-plus.ec.europa.eu/programme-guide/part-b/jean-monnet-actions

Jean Monnet actions in the field of higher education: https://erasmus-plus.ec.europa.eu/programme-guide/part-b/jean-monnet-actions/higher-education

More information:

Erasmus+ (EU programme for education, training, youth and sport) (2021-2027): https://www.eacea.ec.europa.eu/grants/2021-2027/erasmus_en

Erasmus+ Programme Guide: https://erasmus-plus.ec.europa.eu/erasmus-programme-guide

Jean Monnet Actions: https://erasmus-plus.ec.europa.eu/programme-guide/part-b/jean-monnet-actions

Jean Monnet actions in the field of higher education: https://erasmus-plus.ec.europa.eu/programme-guide/part-b/jean-monnet-actions/higher-education

Jean Monnet Activities - Database from 1995 – 2021: https://www.eacea.ec.europa.eu/grants/2021-2027/erasmus/jean-monnet-activities-database_en

For notes

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

____

Course “Activism in cyberspace as a hybrid threats counter”.
Academic year 2023-2024. Didactic materials.
Ed. Serhii Ishchuk, Tetiana Sydoruk, Dmytro Shevchuk,
Olena Shershnova, Kateryna Yakunina. Ostroh 2024. 92 p.

Format 42x30/4. Mind. printing. sheet 4. 100 ave.
Offset paper. Digital printing. «Colibri» typeface. 96 p.

Print by Mariia Svynarchuk
+38 068 68 35 800
print35800@gmail.com