When technology shapes the world

Jared Cohen

In Politique étrangère 2019/1 Spring Issue, pages 121 to 131
Publisher Institut français des relations internationales

ISSN 0032-342X
ISBN 9791037300003
DOI 10.3917/pe.191.0121

When Technology Shapes the World

By **Jared Cohen**

Jared Cohen is the founder and CEO of Jigsaw, a technology incubator within Alphabet and an adjunct senior fellow at the Council on Foreign Relations.

New technologies, particularly in cyberspace, have a strong impact on international relations and conflict. Malicious actors, be they states or non-state actors, have developed sophisticated means of influence. They tend to coordinate their physical and cyber activities with ever-greater precision. The security strategies of Western states need to change as a result and cease operating in silos.

politique étrangère

With the development of increasingly sophisticated yet accessible cyber technology, boundaries are blurring between formerly discrete categories of international political interaction, requiring a reframing of the potential avenues for interstate conflict. Most importantly, states can no longer afford to view physical and digital landscapes as separate. The implications of cyber technology have introduced new threats, necessitating a far more holistic approach to security. In particular, technology has expanded the parameters of traditional warfare, enabling and empowering the individual with the ability to affect the stability of states and the broader system.

This article opts to focus more specifically on influence operations, including disinformation, because this offers the best lens through which to explore the question of how technology is affecting geopolitics. Influence operations, amplified by the power of cyber, are increasingly proving to present novel effects on international interaction. These effects are substantial, yet subtle, and are proving far more difficult to counteract than traditional forms of cyber warfare. Further, the intended target is the psyche of the nation's citizenry, creating unprecedented challenges for governments.

Over the last half century, cyber warfare has reshaped the nature of international conflict and security. The low cost and attribution challenges of offensive action conducted through cyberspace have emboldened both

state and non-state actors. Traditional kinetic warfare has relied upon conventional weapons and targets, which typically constitute the opponent's military, such as destruction of infrastructure and the occupation of a physical space. This has meant that battlefield tactics are developed for contexts of engagement between two or more states in open confrontation. However, the introduction of novel cyber and digital techniques has enabled the pursuit of new objectives, which alter what it means to control a space or effectively win in a conflict.

The primary targets of the cyber toolkit – which include (but are not limited to) tactics such as hacking, malicious software (malware) and denial-of-service (DoS) attacks – have been the penetration, damage and disruption of computers and networks. A further complication is the vulnerability introduced by the near ubiquitous reach and reliance of modern communication technologies, including mobile phones, social networks, messaging apps, and the plethora of devices we have lumped into a category described as "the Internet of Things". The domain of cyber provides a direct line of access between malicious actors and individuals. This creates a readily accessible tactic of destabilization for adversarial governments and non-state groups: their opponent's citizenry.

Although defense departments around the world have invested heavily in systems, weapons and technology to detect, intercept and counteract offensive kinetic and cyber measures, they have not yet begun to fully comprehend this newest conflict front nor properly contemplated how to build resilience and deterrence. This is evident from the lack of consistent policies both at the state and international level, surrounding what constitutes an attack worthy of condemnation or retaliation in the cyber domain. Even in those countries that have identified the importance of anticipating these future threats, efforts are frequently outsourced to the private sector, with minimal coordination, leading to disjunctions between policy and best practices.

When considering the tactical and operational levels of traditional warfare, which have often involved the targeting of physical landscapes or infrastructure, cyber technology introduces new possibilities. It lessens the need for physical engagement by instead providing the psychological capability to leverage citizens to attack their own state. This increases incentives for engaging in cyber activity as a primary or initial method, as it forgoes costly kinetic action by substituting it for the advantages of a nuanced approach of information operations. Cyber technology is therefore changing the calculus and activities of states, especially as evidenced by the evolving advancements in information operations.

It is important to note that these changes do not mean that we are entering a new international system or era; quite the opposite, we are still firmly rooted in the Westphalian model. Rather, our old operating system is undergoing what looks more like a forced upgrade that disrupts the incumbents and elevates those state and non-state actors that rely on asymmetric tactics. The resulting novel features have important implications for future means of conducting interstate conflict and how we ought to be rethinking security in light of the novel hybrid nature of these forthcoming threats.

Technology and the activation of the individual

In analyzing the broad impacts of cyber technology, the most important yet often overlooked impact on geopolitics is its ability to empower the individual. The attributes of the digital landscape, constituted of technology such as peer-to-peer information-sharing and mobile messaging, are enabling the activation of the individual in the international system. As a consequence, the newest wave of geopolitical change is the capacity to command systems of people, galvanized by the interactions they have and the information they consume online. By means of the access and influence afforded by the internet and associated technologies, states and politically motivated groups are granted the ability to create bases of support without individual political figures or any overt involvement.

In particular, disinformation seeks to mobilize individuals towards certain objectives, expertly crafted with the intention of eliciting specific emotional responses in targeted demographics. Information operations deploying cyber technologies have become adept at creating and shaping online networks, which can manifest into broader perceptions of an issue or physical mobilization.

Enhancing this activation, cyber technology also introduces the capacity of a distributed network, coordinated action among a diverse set of actors who may not have experienced any direct interface, minimizing the need for centralized coordination and physical proximity. These dispersed networks are ideal for clandestine operations, hiding within the noise of the vast cyber landscape and lacking obvious connections despite synchronization.

Comprehensive security

States in the international system have traditionally relied on specific conceptual frameworks to think about security, focused on making themselves more resilient to physical military threats. While many states have

adopted and incorporated increasingly sophisticated methods to mitigate cyber threats, most have neglected hybrid threats and future possibilities for overlap. Amplifying this resilience involves consideration of new vulnerabilities in various areas of geopolitical consequence. Malicious use of cyber technology by interfering states has exhibited the potential to erode the democratic system, fomenting chaos and mobilizing groups to destabilize communities and societies at large. Further, as the use of cyber technology as a potential weapon becomes ubiquitous, the risks posed by terrorist and criminal organizations will increase. Cyber has also resulted in a shifting perception of media and problematized ensuring credibility. A lack of coherent policy or articulated rule of law regarding appropriate use of cyber force further complicates international responses to instances of misuse of the technology.

Most states have neglected hybrid threats

In particular, and as will be discussed in the sections below, information operations are adept at exploiting the lack of resilience across these various areas, especially in the capacity to harness psychological vulnerabilities. Neglected in this conversation of resilience and security is the individual, with little consideration given as to how to make individuals more resilient to technological threats specifically designed to stoke their sentiments and behaviors. As the threats evolve along a continuum of individual activation, so too must our models of building resiliency. This continuum describes the varying degrees of sophistication, coordination and network size, from individual efforts to the formal structure of state-run cyber divisions, referred to here as "digital paramilitaries".

This all points to a need to consider a spectrum of resiliency, constituted of vulnerabilities in the physical, digital, and information landscapes. The biggest mistake made by national security architects is the separation of these landscapes. Rather, states are increasingly facing hybrid problems across a variety of geopolitical categories, affecting the nature of elections, political violence and interstate interaction. Thus, we need to now consider the concept of comprehensive *security*: an integrated approach to physical/digital threats and resiliency. This involves considering the role and importance of the individual, which has been amplified by the power of technology.

Technology trends

First and foremost, cyber technology has increased the destructive and destabilizing capacities of malicious state and non-state actors. They have several tools at their disposal. Much of them can be readily acquired on

the deep and dark web, which offers a marketplace of capabilities to actors who otherwise might lack the technical capacity. With this proliferation, actors no longer need to be experts and can instead opt to outsource. This reduces any prohibitive barriers to entry, enabling a diverse set of threat actors to carry out more specialized actions, and increasing the range of potential threat repertoires. Further, developments such as chat-bot automation, which reduces the need for physical manpower to run fake accounts, increase operational capacity.

Additionally, machine learning-powered content generation is increasingly important in facilitating nuance at scale. An important aspect of the disinformation amplification process is to generate different content, but all oriented around a particular theme or specific message, for bots to disseminate to as vast a network as possible. This process is aided as machine learning grows more sophisticated in capturing linguistic nuance. In the future, it will become increasingly more difficult to distinguish between real and fake accounts, and easier to use machine learning to amplify the efforts of an individual, making one person seem like a thousand. It is of vital importance to account for the changing scale of attack, which is shifting dramatically along with technological improvements.

The task of establishing bona fides for inauthentic online personas has constrained state-sponsored efforts to infiltrate and influence local communities abroad. One of the challenges has been in furnishing faux accounts with the visual assets expected of a real individual, which would include attributes such as profile pictures, selfies and photos of friends and family. Thus, malicious actors are often required to use likenesses stolen from real accounts to build up fake identities, leaving these perpetrators open to possible detection. Indeed, the key giveaway of Iran's recently exposed online information operation was their use of fake Twitter accounts developed using images stolen from elsewhere on the internet.[1] While this might be a current limiting factor, AI researchers are making great strides in training algorithms to generate images of entirely fabricated faces.[2] The breakthrough in photorealistic and customizable synthetic image generation appears set to increase the ease of plausible fake account generation.

1. "Suspected Iranian Influence Operations: Leveraging Inauthentic News Sites and Social Media Aimed at U.S., U.K., Other Audiences," *FireEye*, July 13, 2018, available at: <www.fireeye.com>.
2. T. Karras, S. Laine and T. Aila, "A Style-Based Generator Architecture for Generative Adversarial Networks" *arXiv preprint arXiv:1812.04948*, 2018, available at: <https://arxiv.org>.

When considering the activation of individuals, there are particular technological aspects that help to support this potential. The first includes the particular patterns of news consumption, wherein individuals rely predominantly on online resources and social media sites. This has increased the frequency of exposure to novel media and the ease of both distributing and sharing disinformation. The structure of such sites has encouraged malicious actors to use these platforms as primary tools of propagation, relying on peer-to-peer information-sharing models. This is a means to streamline and control traditional kinship networks of information evaluation, relying on the psychological phenomenon wherein people are more likely to believe information given to them by people they know and trust.[3]

This effect is exacerbated by widespread mobile device penetration, rendering most citizens vulnerable to the influence of information operations. Further, mobile messaging is both heavily encrypted and intimate, rendering it ideal for information operations in terms of its access to individuals and its constraints to intelligence and threat monitoring. Counter-operations are generally difficult, given the sheer amount of data being generated.

Activating networks and adeptly manipulating individuals

With this increased capacity for coordination and ease of hiding one's identity, the threat of digital paramilitaries has emerged. These state-sponsored groups develop fake identities that are used to build influence across various social media platforms for use in controlling the online conversation. These groups are a key tool in the activation of networks, subtly and adeptly manipulating individuals towards a particular end goal.[4]

Compounding these threats is the power of disinformation itself, now expertly crafted and propagated by malicious actors with intended behavioral goals. Disinformation is increasingly supported by various tools. One such tool is the promise of synthetic media and deepfakes, which have the potential to help bolster false narratives that undermine political stability. This technology relies on databases of prior recordings of a given individual, and is able to transpose their likeness into fabricated situations which appear incriminating. This is further made credible by technology with the capability to replicate the voice of an individual, resulting in the

3. American Press Institute, "'Who Shared It?': How Americans Decide What News to Trust on Social Media," March 20, 2017, available at: <www.americanpressinstitute.org>.
4. J. Cohen, "Confronting Hybrid Warriors and the Disinformation Tactics They Use," paper delivered at the Aspen Strategy Group, August 2018.

ability to make new recordings that can be attributed to the desired target.[5] With the development of synthetic media, trust in the political system may deteriorate, with false media attributed to a given politician and real evidence being described as fake.

Fake accounts and profiles that propagate false narratives are limited by the scope of what they are able to credibly develop. For example, Russian intelligence and information operation agencies are geographically constrained by the language and content capacity of their officers. While this has led to successful Russian activity in predominantly English or Slavic language-speaking contexts, they are limited in their capacity to influence other regions. Jigsaw has noted French accounts run by Russian agents, but the large language barrier rendered the accounts ineffective and lacking in believability. Despite these current limitations, the international community ought to anticipate the potential future capabilities of content-generating artificial intelligence. As AI becomes increasingly sophisticated, these malicious actors won't need language and culture experts, instead relying on technology to mimic the necessary knowledge base.

While there is a clear understanding of what it means to protect and occupy a physical space in the context of security, this is less clear when considering cyberspace. What would it mean to protect a given section of cyberspace frequented by individuals of a specific nation? There are minimal geographic constraints on activities, with the possible caveat of state-controlled internet. However, those states that have instituted any form of information censorship often do so as part of broader authoritative policies rather than for purely security reasons. Therefore, traditional models of security cannot be transposed into this context; how does one "control territory" in a cyber landscape and win the information battle? There remains a clear issue of how states should ethically wield control or influence in the cyber domain, especially in response to efforts aimed at individuals rather than the state as a whole.

Impact analysis

International relations

In considering the impact of cyber technologies on the international system, one must account for the ways in which it has altered how states relate to one another. The nature of the cyber landscape results in spillover effects spanning across borders, as well as presents challenges for what it

5. "How Lyrebird Uses AI to Find Its (Artificial) Voice," *Wired*, October, 2018, available at: <www.wired.com>.

means for a state to exert control over a space. Further, the pervasiveness of cyber has resulted in the rise of the private sector as new and powerful agents in the international system. The private sector originates this technology and can act as a useful partner, equipped to anticipate or understand potential consequences. As the global community seeks to tackle its largest geopolitical challenges, including extremism in all its forms, political polarization and the orchestration of social movements that seek to destabilize, it is imperative that policymakers account for the galvanizing impact of cyber technology. Cyber technology is rewiring the architecture of the state, with important effects for international systems, presenting new demands and challenges that existing paradigms are poorly equipped to meet.

In the context of Ukraine, cyber technology and disinformation efforts are being wielded to undermine the state's reputation abroad and the integrity of its alliances. The Russian disinformation and cyber campaign has aimed to suffocate Ukraine by alienating it from surrounding countries. Disinformation narratives have been aimed at isolating[6] Ukraine and portraying it as an adversary,[7] in addition to provoking historical tensions.[8] This has included attempts to make Ukraine a political liability for its allies by tarnishing its reputation, in part by promoting news that portrays Ukraine as antithetical to Western ideals and norms. More specifically, this has included supporting the activities of militant/neo-Nazi groups in western parts of the country under the guise of Ukrainian accounts, and promoting news of attacks on minority populations living in Ukraine (especially Polish, Hungarian, Romanian, Roma[9]), prompting responses from foreign governments. While some of the news propagated is true, some Ukrainians contend that this information would not be as widely publicized were it not for the activities of Russian operatives on the ground, documenting and promoting this information globally. The intended purpose is to undermine Ukrainian collaboration with neighboring states, especially EU member nations. Russia is seemingly threatened by the prospect of a more formalized relationship between Ukraine and the EU, which could supplant Russian influence in the region. Coupled with more overtly aggressive kinetic action, cyber and disinformation activity introduces a subtler dimension that is unlikely to provoke a response

6. "More and More ISIS Fighters are Coming to Poland from Ukraine, Therefore a Wall Has to Be Built on the Border," January 2016, *EU vs. Disinfo*, available at: <https://euvsdisinfo.eu>.
7. EU vs. Disinfo, "Poland, Hungary, and Romania have Territorial Claims Against Ukraine," February 2016, *EU vs. Disinfo*, available at: <https://euvsdisinfo.eu>.
8. G. Baczynska, "Poland Says War-Time Killings Tarnish Ties with Ukraine", Reuters, July 2018, available at: <www.reuters.com>.
9. "Ukraine Roma Camp Attack Leaves One Dead," BBC, June 2018, available at: <www.bbc.com>.

from the international community. This strategy has already proven successful, with the Netherlands rejecting closer EU ties to Ukraine in a 2016 referendum.[10] In the future we ought to anticipate the ability of cyber technology to affect the factors influencing perceptions within the international system, as well as the potential stability of the current status quo relationships and interactions.

Domestic governance

Disinformation plays an important role in shaping the perspectives, opinions, and behavior of ordinary citizens, with potentially destabilizing consequences. Information operations that use the tools provided by cyber technology introduce an ability for actors to effectively disrupt traditional systems of domestic governance.

As mentioned above, tools taken from the deep/dark web, especially convincingly doctored videos, have the potential to undermine credibility in the very system of governance, obscuring and disrupting individual ability to identify the truth.[11] While there is certainly an extensive history of states attempting to engage in foreign election interference, cyber technology introduces the capacity for more nuanced approaches. The primary lever through which the desired impact is achieved is the activation of the individual.

This activation can vary in its level of sophistication. As evidenced by Russian attempts to interfere in the 2016 US election, this application of covert information operations involved highly organized teams charged with targeting particular demographics. These teams of state-sponsored cyber groups tasked with destabilizing foreign adversaries can be labeled as digital paramilitaries. Such groups include the Internet Research Agency, a Kremlin-supported private company which conducts information operations on behalf of Russian intelligence. They have developed several successful accounts on all sides of the political spectrum to promote polarization and societal fracturing. This has included a fake pro-Trump account, @tpartynews, which frequently targeted Black Lives Matter (BLM) activists, and @Blacktivist, which, in addition to more insidious activity, promoted real BLM protests. There have also been documented incidents of advertising purchased on social media platforms to promote a chosen narrative that the Kremlin feels would help it achieve a strategic goal.[12]

---

10. "Dutch Referendum Voters Overwhelmingly Reject Closer EU Links to Ukraine," *The Guardian*, April 2016, available at: <www.theguardian.com>.
11. T. Simonite, "Will Deepfakes Disrupt the Midterm Election?," *Wired*, November 2018, available at: <www.wired.com>.
12. J. Cohen, "Confronting Hybrid Warriors and the Disinformation Tactics They Use," *op.cit*.

The key takeaway from these instances is the possibility of coordinated action across seemingly disconnected platforms and accounts to achieve a particular political goal: in this case, fanning the flames of various domestic political arguments in order to shape election results.

Conflict and War

Much of the conversation on the role of technology in activating the individual has revolved around recruitment and promotion of violent extremism online. In order to anticipate future trends, we ought to rethink how the process of radicalization is supported via technology. This is no longer something committed by non-state actors for translation into kinetic action. For nations involved in warfare, targeted disinformation campaigns are increasingly being deployed as the first strike of a military operation, representing a fundamental change in how conflict emerges and develops.

In Ukraine's hybrid conflict against Russia, complicated coordinated actions carried out along multiple fronts, both physical and digital, have added to the fog of war.[13] The disinformation campaign in eastern Ukraine has involved the influence of Russian and pro-Russian media targeting conflict-affected areas and occupied territories. Along the physical frontlines, interference campaigns are coupled with kinetic attacks, with cyber attacks and disinformation used to diminish capacity and the relationship between authorities and civilians. Russia is using organized divisions of digital paramilitary to fill the space with overwhelming disinformation and leverage fake accounts to instigate chaos.

The cyber and disinformation tactics employed by both Ukrainian and separatist forces are creating an added layer of complexity to the physical conflict. One popular disinformation story involved the apparent crucifixion of a young boy by Ukrainian forces, which was disseminated with the goal of depicting the Ukrainian army in a negative light to undermine foreign support.[14] A newer trend in coordinated Russian behavior has involved blocking accounts, especially those of Facebook users or bloggers, by sending large numbers of complaints in order to persuade a website to take them down. This is an effective means of taking control of the online conversation by stifling dissenting voices. Russia is also finding and capitalizing on sensitive moments in the history of a given account to exploit for the purposes of instituting a ban. Analysts in the region are also

13. A. Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired*, June 2017, available at: <www.wired.com>.
14. A. Nemtsova, "There's No Evidence the Ukrainian Army Crucified a Child in Slovyansk," *The Daily Beast*, July 2014, available at: <www.thedailybeast.com>.

noting Russian use of Telegram to create influential groups or propaganda channels to discredit Ukrainian military efforts, complicating traditional "hearts and minds" approaches to dealing with militant- or separatist-supporting civilian populations. They have also seen hundreds of channels coalesce around a particular topic or narrative, such as the recognition of the Orthodox Ukrainian church.[15] It is also important to note that, while much research and focus has been directed in the West at more prolific platforms such as Twitter, Facebook and YouTube, there is a clear need to focus on other popular communication platforms, including WhatsApp, Telegram, and Signal. This is especially clear in the context of Ukraine, where much of the malicious activity is conducted over these sites.

Stifling dissenting voices

In response to this threat, Ukraine has developed its own militarized disinformation wing, tasking individual soldiers with a typical load of 30 to 40 accounts. Each analyst is relatively autonomous, relying on previous instruction regarding how to respond to a specific pattern or trend in online behavior, and engaging in more precise messaging borne out of circumstance, adapting to the situation.

Information operations have developed general archetypes of individuals from different geographic areas and demographics, which guide account fabrication and inform commenting behavior to increase perceived authenticity. Typically, the profile is not too in-depth, the reason being that, among hundreds of comments on a particular post or profile, people are unlikely to check or investigate a given "fake" profile. Technology is also assisting in routine or traditional activities: Ukrainian forces are heavily reliant on local intelligence, which is received over the internet, telephone, and Telegram/WhatsApp/Viber messenger apps. The importance of social media cannot be overstated; even the Ukrainian military is focusing its monitoring activities on larger social media platforms targeting specific news websites.

Current counter-trolling is manual rather than automated, employing a call-center model, which puts it at a large deficit when compared with Russian technological capacity. The typical strategy involves finding an article disparaging the Ukrainian government, which is being promoted as a result of Russian involvement, and then diminishing its prominence or promotion on a given site. The Ukrainians suffer from a lack of resources

15. S. Wemer, "Ukrainian Patriarch Warns Russia Will Exploit Split in Orthodox Church," *Atlantic Council*, September 2018, available at: <www.atlanticcouncil.org> and K. Kruk, "The Last Missing Piece to Make Ukraine Truly Independent," *Atlantic Council*, August 2018, available at: <www.atlanticcouncil.org>.

to adequately respond to the threat. Military officials are now calling for a more holistic, country-wide response, stating that if the military is the only one responding to the problem there will be no strategic result. This requires the involvement of state and local authorities to complement ongoing military effort. Russian media engage in precise messaging, which contrasts with the diversity of Ukrainian media when reporting on issues. Ukrainian military officials feel that the information war cannot be won through playing by a different set of rules than their adversary and that the solution is some form of censorship or control over the media.

The Ukrainian military has witnessed clear, sophisticated coordination of cyber and physical behaviors. Russians will opt to first engage in a cyber response either by providing disinformation preparation for military action or by engaging in cyber attack to immobilize the enemy. One permutation of such coordination may involve preliminary Russian engagement in a kinetic attack, followed by dissemination of an argumentation rooted in disinformation explaining the event. Physical action might also be coupled with a cyber attack, rendering Ukrainians incapable of commenting on or responding to the event, thus further undermining their credibility among the local population. One such example could include Russians posting online the likelihood of a kinetic action without any concrete details, then proceeding to block accounts, then conducting provocative military action, which would elicit a reaction from the Ukrainian side, and finally, given the prior announcement, blaming Ukrainians for causing it. The combined cyber/kinetic component of the war renders the population "emotionally ready to buy disinformation as true".

The power of cyber technology is not limited to state actors. While ISIS currently occupies global imagination as a formidable group capable of challenging international order, it is worth noting the possibility of the destructive capacities of a similarly structured group supported by a cyber division. An important question to consider is what the cyber capacity of a future ISIS would look like. While the academic and political community is focusing heavily on the role of cyberspace in aiding recruitment and facilitating the reach of propaganda, little attention is given to anticipating potential future cyber capacity and the ways in which it might further obscure financing. Occupying physical territory may no longer be enough: a future ISIS could undertake systematic campaign to own the conversation in Raqqa, either as a preemptive strike or in conjunction with kinetic action.

***

Cyber technology has already begun to change interstate interaction and conflict, and has showcased the power it has over the psyche

of individuals, to motivate and control in the pursuit of destabilization. As illustrated, it has a unique ability to enhance the scope of information operations and is offering malicious actors the means to weaponize individuals against their own governments. Given this far-reaching impact, it is imperative to reconsider current siloed models of security, which differentiate between kinetic and cyber force and fail to properly account for the full range of possible vulnerabilities that could damage the state. Rather, what is needed is comprehensive security, which involves accounting for threats resulting from the blending of cyber and kinetic. This lens is necessary in forecasting the *zeitgeist* and paradigms of potential importance in 2020. As cyber continues to develop, so too do the potential challenges and threats. Forecasting the next threat requires building on the horizon and looking to the right contexts for evaluation. This entails a fundamental reshaping of how we consider security and what states will eventually be capable of with the help of technology. Beyond states, one must also consider how technology has the potential to be misused by non-state actors and groups to exact harm on a grander scale. Further, given that much of this technology originates in the private sector, we should also ask the question: What does an international security strategy look like for a company? Companies are not currently positioned to be patriotic towards one country, but there is a spirit of patriotism towards the underlying values of the internet.

Cyber technology presents both unique opportunities and challenges, all of which have massive consequences for the integrity of the international system and the states within it. Its continued evolution requires a contiguous evolution in our approach to security, future threats, and methods of conflict.

Keywords
Cyberwar
Social networks
Disinformation
Propaganda