Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

ISSUE BRIEF

Collective Defense of Human Dignity: The Vision for NATO's Future in Cyberspace

JULY 2019 CHRISTOPHER B. PORTER

OVERVIEW

As it celebrates its seventieth birthday, NATO is an alliance under tension.[1] It must face the challenges of burden sharing, an emerging multipolar world of old adversaries and new challengers, and the perception of the Alliance in the domestic politics of its member states. In cyberspace, NATO member states are pulling in different directions on cyber defense policy and planning. For example, on the issue of Chinese investment and deployment of high-speed 5G cellular networks, various NATO members are going their own way to either encourage, allow, slow, ban, or stop the spread of Beijing's technological dominance, as information infrastructure has emerged as a new domain of both economic competition and national security risk. Often, dialogue on these issues devolves into allies talking past one another, without a shared basis of facts with which to frame a debate. Yet, Alliance members still share indisputable common cyber threats—Russian information operations, the possibility of catastrophic disruptions to the global financial system, and increasingly dangerous non-state actors—that all allied nations seek to work more closely together to combat. Moreover, NATO members share a desire to work together at more than just a force level: NATO is an alliance in search of a vision for cooperative action in cyberspace that can defend common values of human dignity and a desire for global peace, using methods that reflect the values of respect for the rule of law and state sovereignty.

NATO is evolving on joint cyber defense at the exact moment that the nature of operations in cyberspace is itself changing. Cyber operations are increasingly militarized. Capabilities previously used exclusively for

The Scowcroft Center for Strategy and Security works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

1 Ashish Kumar Sen, NATO Engages: The Alliance at 70, Atlantic Council, April 1, 2019, https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-engages-the-alliance-at-70.

NATO Cooperative Cyber Defence Centre of Excellence *Photo credit: ARRA3231/Flickr*

cyber espionage are more and more often used instead as the first staging grounds for disruptive or destructive cyberattacks. Militaries no longer reliant on tools borrowed from spy agencies are now in command of their own cyber capabilities and have institutional momentum to engage in shows of force. Non-NATO governments increasingly release intelligence gathered via cyber means to the public, to impugn reputations and disrupt adversary governments. Messaging between rivals happens as often via social-media-driven propaganda campaigns as through diplomatic backchannels. All of this is happening while placing civilians and privately owned networks—rather than uniformed armed forces and the government networks NATO is focused on defending—on the front lines.

In recent years, the Alliance has taken positive steps to bring NATO cyber-force projection and cooperative-defense policy in line with the new realities of war in the information age.[2] Since agreeing in 2014 that a cyberattack could trigger Article 5 collective-defense responsibilities, NATO leaders have worked to improve national-level defense of digital networks necessary for military interoperability, and to recognize cyberspace itself as a domain of military conflict. The NATO Cyber Defence Centre of Excellence has continued to provide excellent training, education, and thought leadership on all aspects of Alliance joint cyberspace defense and operations. While NATO does not have its own cyber capabilities, common exercises and cross-training programs have spread practical knowledge and opportunities for increased jointness within the Alliance, and a new NATO cyber command to combine member

2 Laura Brent, "NATO's Role in Cyberspace," NATO Review, February 12, 2019, https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm.

states' deterrent efforts is planned to be fully staffed by 2023.[3] Outside of formal Alliance structures, the US Cyber Deterrence Initiative—announced by the White House in September 2018—promises to build, on an ad-hoc basis, a "coalition of like-minded states" that will "coordinate and support each other's responses to significant malicious cyber incidents." This will no doubt, from time to time, include many NATO members in attributing and imposing "consequences against malign actors."[4] The private sector, too, is playing an important role within the Alliance—providing technical training, facilitating unclassified threat-intelligence exchanges between members, combatting disinformation online, and improving force readiness.

At this turning point in Alliance history, the Atlantic Council convened a dinner meeting at the Munich Security Conference on February 15, 2019, where leaders from governments throughout the Alliance, crucial private-sector partners, technical experts, and thought leaders from nongovernmental organizations could meet to discuss common problems and find a driving force for a way forward together. Participants raised and discussed several critical questions.

- What are the prospects for a peaceful resolution to cyber conflict between NATO and leading sources of threat, such as Russia?
- How can Alliance members with radically different cyber capabilities work together, especially on joint-attribution statements that might lead to lethal conflict?
- What role should the private sector play in making war and peace in cyberspace alongside states?
- What should be done about China, seen variously by members states as a potential partner in prosperity and peace, a sometimes-predatory economic rival, and a potential future adversary in great-power conflict?

The event was titled "Defending Human Dignity: Limiting Malicious Cyber Activity Through Diplomacy." Fittingly, the most important question of the night was this: in a struggle that remains below the level of armed conflict, what is the rationale for NATO common defense in cyberspace? Does it exist to protect governments or people, or should it be centered on defense of certain values? If the latter, what values do NATO members hold in common that are threatened in cyberspace by shared adversaries?

VALUES-DRIVEN STRATEGY NECESSARY TO MUSTER ALLIES' WILL TO FIGHT

"The Parties to this Treaty reaffirm their faith in the purposes and principles of the Charter of the United Nations and their desire to live in peace with all peoples and all governments.

"They are determined to safeguard the freedom, common heritage and civilisation of their peoples, founded on the principles of democracy, individual liberty and the rule of law. They seek to promote stability and well-being in the North Atlantic area.

"They are resolved to unite their efforts for collective defence and for the preservation of peace and security."

— Preamble, North Atlantic Treaty of 1949

NATO was created in the face of military and political threats to the existence of European governments posed by an expansionist Soviet Union: "events such as the Berlin blockade in April 1948, the June 1948 coup in Czechoslovakia and direct threats to the sovereignty of Norway, Greece, and Turkey."[5] Yet, NATO's founding document clearly points to the Alliance's fundamental raison d'etre: not to defend particular governments, but to defend civilizations in the North Atlantic born from the principles of democracy, individual liberty, and the rule of law.

3 Kurt Rauschenberg, "Maryland Guard, Estonian Service Members Conduct Cyber Exercise," US Department of Defense, May 21, 2018, https://dod.defense.gov/News/Article/Article/1526872/maryland-guard-estonian-service-members-conduct-cyber-exercise/; Robin Emmott, "NATO Cyber Command to Be Fully Operational in 2023," Reuters, October 16, 2018, https://www.reuters.com/article/us-nato-cyber/nato-cyber-command-to-be-fully-operational-in-2023-idUSKCN1MQ1Z9.

4 "National Cyber Strategy of the United States of America," White House, September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

5 "Founding Treaty," NATO, last updated January 30, 2017, https://www.nato.int/cps/ua/natohq/topics_67656.htm.

Today's most pressing cyber threats to member states in the North Atlantic directly target these principles as a means of undermining entire civilizations—first, as a precondition for political change, and possibly in lieu of military conflict altogether. Russian, Iranian, and Chinese cyber operations have all, to varying degrees, aimed to undermine confidence in free and fair elections, or to alter election outcomes in Europe and North America. Those governments, and others, have suppressed freedom of speech, the free practice of religion, and free assembly at home, as well as within NATO countries through the aggressive use of cyber espionage, information operations, and online harassment targeted at expatriates, religious and ethnic minorities, journalists, and critical academics. Cybercriminals are sheltered and given license to disrupt, destroy, or steal from networks in rival nations. In some cases, state-sponsored cybercriminals blur the line between government and goon in ways that erode public confidence in international law enforcement.

Several dinner attendees felt that defending human dignity was the key mission for NATO cyber defenders. While London and Beijing both make extensive use of surveillance cameras and automated systems to track potentially threatening behavior, the United Kingdom's rule of law and privacy protections make that deployment of technology fundamentally different than China's potentially coercive uses. Concerns about the nature of free persons in relation to a large, wealthy, technologically advanced state also pervaded the evening's discussion of cyber operations. Through that lens, large-scale collection of private digital data—while still a concern in the West, because of the potential for abuse of civil liberties—takes on a directly threatening dimension when Russia or China engages in such behavior, because of the likelihood that such information would be used for blackmail, propaganda, or other purposes unnecessary for legitimate state security and contrary to human dignity.

These operations are more than just a nuisance to be endured or a crime to be prosecuted. Taken together, they risk undermining not only the way of life for millions within the North Atlantic states, but the very legitimacy of those states. Indeed, these tyrannical uses of cyber operations occupied most of the evening's discussion, and were the feared flashpoint for long-term NATO cyberconflict, in contrast to attacks on government networks or critical infrastructure, or the applications to the conventional battlefield that normally pervade government-run strategic discussion within the Alliance. Ironically, the highest strategic and moral priority revealed in these discussions is currently one of the lowest priorities for NATO members.

CHINESE 5G NETWORKS A CURRENT TEST OF ALLIANCE VALUES

This concern extends into future theoretical conflict, and directly applies to pressing security issues currently bedeviling the Alliance. The explosive expansion of Chinese government-backed 5G telecommunications networks, for example, elicits very different reactions from leaders within NATO depending on their framing of the issue. As an economic issue, the United States and a few other technologically advanced states have pressed very hard for Alliance members to purchase from one another, often conflating trade and security issues in ways the United States has historically avoided. For many smaller and less wealthy member states, China's offers of cheaper equipment, generous subsidies, and extensive personnel support make the use of Chinese-origin 5G networks an economic reality and practical necessity.

From a security standpoint, the United States and its "Five Eyes" partners Canada and the UK, as well as Poland, have expressed extreme concern about Beijing's potential to leverage the deployment of 5G technology for espionage purposes. These concerns have grown severe enough that senior US officials have stated that the mere presence of Chinese-origin technology could undermine future NATO interoperability. In the absence of hard evidence shared by the United States that Chinese plans, or even has the capability, to conduct such operations, many member states have responded to these concerns with something between a shrug and a plan to isolate Chinese equipment away from the core of their telecommunications networks and military secrets. None has so far expressed serious interest in spending billions to replace Chinese equipment with European or US alternatives, much less to pass unpopular mobile-bill increases onto their citizens based on what still seem like abstract concerns. Nevertheless—if these security concerns are later proved legitimate—the longer hosting countries wait to act, the more difficult and expensive it will be to amputate compromised technology from national infrastructure.

These discussions are unproductive, in no small part, because they are unmoored from shared values and too focused on specific tactical concerns. Democracies should not rely on free speech provided at the whim of an authoritarian government. A military alliance in which one or several members might reasonably foresee engaging in armed conflict should not rely on critical infrastructure provided by a future military rival. Citizens in a free country should not have their access to information services controlled by a foreign power that could restrict that access in a time of political or military conflict. Backdoors created by a rival might be exploited not only by them, but by likeminded countries, such as Russia, that pose a more proximate military threat to the heart of the Alliance.

According to many attendees at the event, NATO should be skeptical of China's 5G ambitions, but such skepticism ought to be anchored in a risk-management approach, rather than the current security paradigm that ebbs and flows with each revelation of new vulnerabilities. Absent a shared Alliance emphasis on the values being defended, however, it is hard to justify such risk management when the immediate benefits of buying cheaper equipment are clear, and the downside is only a future that members have not yet agreed they want to fight to prevent.

For NATO, success on 5G looks like a world in which the Alliance's networks are secure, their control and operation are transparent to users, and maintenance and policy decisions are made using Alliance countries' personnel. China insists on these same standards for its own networks as a means of maintaining government control and security; NATO ought to do the same as a means of protecting human dignity and Alliance-wide freedom and prosperity.

COMPETING SYSTEMS HAVE BEGUN FRACTURING THE WORLD

Attendees made a variety of observations about the nature of competition between NATO and its potential rivals, most notably China, best summarized by the description of these conflicts as "systems competition." In this kind of competition, specific threats rarely become security matters that rise to the level of Alliance consultation. China's state-controlled capitalism, with its emphasis on technical innovation and wealth generation—absent the development and spread of democratic norms and values that accompanied Western systems in the past—is naturally attractive to developing nations in search of alternative governance models that might allow them to retain greater centralized control. But, Beijing's trade network has also spread through the heart of advanced democracies looking to jumpstart economic growth or partner and benefit from the next technological breakthrough.

This apparent conflict between a global free-trade model in which integration with other countries is a goal rather than a risk, and the very real security challenges that come from engaging in trade with an economic behemoth that does not share the values that undergird that system, is becoming more apparent every day. While this event was primarily concerned about cyber and other high-tech threats, many attendees expressed similar concerns about the risks of Chinese ownership of ports, sales of railway cars and equipment, and civil aviation dominance—all viewed as unhealthy on the whole, but making economic sense in each particular instance.

These rapid changes in allegiance—looking to the US-led world order for security and democratic values, and to China's system for an investment boost—are only going to accelerate as the pace of technological change intensifies, increasing the risk of fractures within the Alliance. Nowhere are the stakes of this division higher than in the emerging field of artificial intelligence, where societies endeavor to make machines that can think for themselves, while doing so from within the framework of each society's own values. The challenge for human beings will be to ensure that machines remain accountable to people, with an emphasis on reserving decisions that only humans can make, but this will be complicated if key elements of innovation in artificial intelligence occur within a Chinese state-controlled system with very different ethics regarding privacy—autocracies are natural data aggregators—and individual human dignity and rights.

NATO ALSO NEEDS A PLAN FOR PEACE

Attendees almost universally expressed a belief that defending these values did not mean that conflict with Russia, China, or other rival powers was inevitable. Those nations primarily act in cyberspace to enhance their domestic security and economic power, rather than to spread an ideology per se. To the extent that NATO's core concerns remain defense of Western freedoms and values among the member states, there is

FBI Executive Assistant Director Amy Hess speaks at a November 28, 2018 press conference at the Department of Justice announcing charges against two Iranian men in connection with an international computer hacking and extortion scheme involving the deployment of sophisticated ransomware known as SamSam. *FBI.gov/Department of Justice*

room to negotiate peaceful resolutions to cyber conflict with those rivals. Agreements that improved the domestic security of those rivals would, in many ways, be a positive outcome for NATO in its own right, because the increased confidence that might come with improved security would reduce much of the logic for disruptive foreign aggression.

Several attendees, especially those with private-sector backgrounds, expressed deep skepticism about the wisdom of indictments and sanctions as tools of improving cybersecurity. While diplomatic engagement with countries that sponsor cyberattacks has produced tangible gains for individuals and companies in terms of the rate at which they suffered cyber intrusions, over time, the practice has become politically unpopular. What was thought to be the eternally popular policy options of indicting foreign nation-state hackers and sanctioning sponsoring governments has shown little or even negative effects on risk for the average citizen across the Alliance.

Attendees expressed several additional concerns beyond the lack of evidence regarding the efficacy of these policy tools. Namely, they shared concerns that the private sector was being asked to support indictments and sanctions without strong evidence to back them. Other concerns included fears that indictments and sanctions were often used to relitigate old crimes, led to economic or diplomatic blowback disproportionate to security gains, and seemed increasingly motivated by political, rather than security, concerns—particularly with regard to China's economic-espionage activity and telecommunications risks. Several attendees noted that the United States needed to return to expressing its security concerns on these issues in a "truth-centric" manner, free from hyperbole, or risk mortgaging its reputation and the faith of other nations in US claims on cyber-threat issues.

NATO should, therefore, remain open to peaceful diplomatic engagement on cyber issues with rivals, especially Russia, as perhaps the best means of improving cybersecurity for citizens and protecting valued freedoms. The most painful part of reaching such

an agreement will no doubt be the necessity for NATO members to restrict their own sometimes-useful cyber operations in line with expectations for rivals, and as a means of demonstrating the Alliance's commitment to defending and living up to its principles worldwide. Several attendees pointed to President Emmanuel Macron's Paris Call as a model for further development of norms in cyberspace, while others felt strongly that bilateral negotiations between major cyber powers were more likely to be fruitful.[6]

Regardless of form, an enforceable agreement that defends NATO values should include;

- zero tolerance for cyber operations that disrupt systems key to democracy, such as election infrastructure or individual parties and campaigns, or that deliberately reveal information obtained by intelligence means to the public as a means of influencing election outcomes or civil society;

- restrictions on targeting of civilian facilities providing care necessary for basic human dignity, such as hospitals, even for espionage purposes, as doing so could open such facilities to disruptive attacks;

- prioritizing the defense of individual citizens' personal information, especially as a means of protecting religious and ethnic minorities and expatriates from exploitation by foreign powers;

- restrictions on certain classes of activity targeting critical-infrastructure facilities during peacetime that go beyond those present under current international agreements; and

- extending restrictions on state-backed theft of intellectual property for commercial purposes to include states beyond the United States and China. As with the US-China agreement, expanded agreements should include greater cooperation on investigating and combatting cybercrime, so that signatories can differentiate between operations that are state-sponsored vice and those simply originating from a state, while also enhancing the Western priority of rule of law.

It is hard to forge international consensus, even between like-minded allies such as the NATO member states. It is even harder when including the non-state, but no less essential, private-sector entities that undergird the Western economy. This makes the tentative consensus of the Atlantic Council's dinner meeting on the sidelines of the 2019 Munich Security Conference all the more meaningful, and highlights the strength of the transatlantic Alliance, which aspires to base itself on enduring principles. While stakeholders at the dinner differed on the details, an inspiring agreement emerged that the Alliance's efforts in cyberspace ought to center around the defense of human dignity, a desire for global peace, and a respect for rule of law. A roadmap remains to be drawn up—and this paper offers only a first draft of one—but Alliance stakeholders appear to agree on the destination. Perhaps the Alliance can reach it over its next seventy years.

Christopher Porter is a nonresident senior fellow with the Cyber Statecraft Initiative at the Atlantic Council's Scowcroft Center for Strategy and Security.

6 "Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace," France Diplomatie, Ministry for Europe and Foreign Affairs, November 12, 2018, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

Atlantic Council | Board of Directors

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org