Information & Security

P. Poptchev
vol. 45 (2020): 35-55
https://doi.org/10.11610/isij.4503

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

NATO-EU Cooperation in Cybersecurity and Cyber Defence Offers Unrivalled Advantages

Peter Poptchev

ABSTRACT:

The article identifies the trends as well as documented instances of adversarial cyberattacks and hybrid warfare against NATO and EU Member States. It illustrates how these adversarial activities impact on the broader aspects of national security and defence, the socio-economic stability and the democratic order of the states affected, including on the cohesion of their respective societies. Cyberattacks by foreign actors—state and non-state—including state-sponsored attacks against democratic institutions, critical infrastructure and other governmental, military, economic, academic, social and corporate systems of both EU and NATO Member States have noticeably multiplied and have become more sophisticated, more destructive, more expensive and often indiscriminate. The cyber and hybrid threats are increasingly seen as a strategic challenge. The article presents some salient topics such as the nexus between cyberattacks and hybrid operations; the game-changing artificial intelligence dimension of the cyber threat; and the viability of public attributions in cases of cyberattacks. On the basis of analysis of the conceptual thinking and policy guidelines of NATO, the European Union and of the U.S., the author makes the case that a resolute Trans-Atlantic cooperation in the cyber domain is good for the security of the countries involved and essential for the stability of today's cyber-reliant world.

ARTICLE INFO:

RECEIVED:	12 SEP 2020
REVISED:	30 OCT 2020
ONLINE:	17 NOV 2020

KEYWORDS:

NATO-EU cooperation, cyber defence, cyberattacks, hybrid operations, U.S. Cyber Security Strategy, national cyber capabilities

✉ E-mail: peter.poptchev@gmail.com

Introduction

The idea of proposing enhanced EU-NATO cyber cooperation at a time when both the European Union (EU) and NATO experience open challenges to their integrity, indeed their very existence, from capitals to the East and to the West as well as from Eurosceptic and populist forces within, might seem untimely. While such doubts are reasonable, a closer examination of the problem, as attempted in this article, reveals that Trans-Atlantic cooperation in the cyber domain is good for the security of the countries involved and essential for the stability of today's cyber-reliant world.

The EU's decision to pursue strategic autonomy, and the increasing NATO-EU security and defence cooperation observed in the last several years in particular, bring the two blocks closer together in well specified areas, not the other way round. The U.S., which under President Trump does not seem to value the EU sufficiently, to say the least, clearly needs allies and partners in at least two critical areas: missile defence and cybersecurity. In the past year, Washington's recurring wish to restore working relations with the new leaders of the EU, as conveyed by Secretary of State Mike Pompeo, is an encouraging sign but with little practical consequence.

In its Cyber Security Strategy, Washington recognizes that many allies and partners possess unique cyber capabilities that can complement their own and sets as a priority action to strengthen the capacity and interoperability of those allies and partners to improve the United States ability to optimize the combined skills, resources, capabilities, and perspectives against "shared threats."[1]

NATO-EU cooperation in cybersecurity and cyber defence, including partner nations around the world, can be highly beneficial as both political interest and technological expediency converge to make a strong case for addressing the common cyber challenge together. This would entail basically two pathways: (1) tackling the cyber threat and related hybrid warfare effectively; and (2) engaging the rest of the world in regulating cyberspace, including related new technologies such as artificial intelligence (AI), Internet of Things (IoT) and 5G.

Both the "defensive" and the "offensive" techniques and procedures necessary for solving the first challenge increasingly rely on governments' capabilities to monitor, detect, analyse and manage big data, including through cross-border exchange, access to deep knowledge and a productive relationship with industry, academia and social media companies. An allied and partner format, involving dozens of countries in well-defined exchange and cooperation streams, is matchless in this regard.

The same applies to the second pathway, which requires multilateral communication and diplomacy vis-à-vis ambitious competitors and adversaries operating in cyberspace, who are however equally, if not more, dependent on scientific and technology exchange and international trade. The Euro-Atlantic community of nations, including partners around the world, share identical strategic interests in the digital era. This group of countries can be—once the necessary international conditions and prerequisites are in place—an influential force, capable of shaping the outcome in any global forum tasked with developing cyberspace rules.

Background

In the run-up to the July 2018 NATO Brussels Summit, a debate was held in several Allied formats on the feasibility of adopting shared principles and capabilities, including perhaps a common strategy, to develop reliable cybersecurity and cyber defence. The debate remained inconclusive, yet it revealed that Allies would be ready to exchange information and cooperate on a voluntary basis, as appropriate. This position was constructively elaborated in time for the Summit to state that…"We have agreed how to integrate sovereign cyber effects, provided voluntarily by Allies, into Alliance operations and missions, in the framework of strong political oversight."[2] NATO thus applies a pragmatic and flexible approach to rallying the national cyber capabilities of Allies and, where applicable, Partners to deter, protect and defend against the common cyber threat acquiring global proportions.

The Brussels Summit reconfirmed that cyber defence was part of NATO's core task of collective defence and emphasized that Allies must be able to operate as effectively in cyberspace as they do in the air, on land, at sea, and in space to strengthen and support the Alliance's overall deterrence and defence posture. The actual implementation cycle—in particular, in acquiring and deploying capabilities to cope with the whole range of adversarial cyberattacks and intrusions—is expected to take several years. The fight against cyber- and hybrid attacks becomes a key component of NATO's 360-degree approach to security.

In anticipation of these developments and based on more than two years of research, a NATO Workshop, entitled "Integrated Approach to Cyber Defence: Human in the Loop," held its concluding session in Sofia in April 2018. The workshop focused on promoting cyber security system thinking and deliberating on how human factors can enhance cyber defence in national and allied format.[3] The workshop posited that the growing complexity of cyberspace, and of the cyber threat itself, requires an enhanced supportive attitude to the role of humans. It also substantiated an integrated approach to cybersecurity and cyber defence, which essentially corresponds to the "holistic" approach to cybersecurity adopted by the EU in 2015.

Not only technology but also knowledgeable and well trained specialists should be treated, on an equal if not enhanced basis, as indispensable to developing proactive cyber systems of deterrence, protection and defence, concluded the workshop.[4] An array of impressive analyses, empirical studies and tested variants of physical cyber systems were presented at the Sofia workshop, demonstrating up-to-date Allied capabilities: from biometric identification schemes used in immigration controls to visualization for cyber situation awareness, to detection of enemy's information injections, to ensuring weapons' or avionics systems' cybersecurity. While the workshop kept to its mandate and highlighted scientific and technical aspects of cyber defence, the multi-faceted analytical findings allowed for a statement in the Technical Evaluation Report of a broader political nature, namely: the expanding complexity of cyberspace, if left unaddressed and unregulated, will create cyber chaos with unpredictable consequences.

This author made a presentation at the Sofia workshop too, arguing that developing a holistic cyber security and cyber defence strategy by collaborative efforts of NATO and EU, through doctrinal alignment and structured coordination, would contribute to addressing effectively the symbiotic challenges of cybersecurity and cyber defence.[5] While some participants found the proposal relevant, the idea of a common EU-NATO cyber strategy was judged premature and did not garner sufficient support.

On the other hand, the decisions taken at the Brussels NATO Summit on cyber defence clearly support the logic that developing, as a minimum, "cyber warfare principles" is absolutely necessary to allow the Alliance to integrate individual nations' cyber capabilities into Alliance operations.[6] The issue has important operational as well as doctrinal aspects, the latter pertaining, in particular, to the possible application of Article 5 in cases of adversarial cyberattacks and/or hybrid operations. The process of developing NATO cyber warfare principles or a similar set of engagement rules should go hand in hand with exploring and operationalizing the potential of a more elaborate EU-NATO cyber security cooperation. At the close of the 2018 Summit, Secretary General Jens Stoltenberg emphasized that NATO was "stepping up cooperation with the EU on cyber defence, military mobility, and in countering hybrid threats."[7]

This article attempts to identify the underlying trends in cyberattacks and hybrid warfare and, in particular, the political and strategic implications of adversarial cyberattacks on NATO and EU Member States' assets. The text further illustrates how these adversarial activities impact on the broader aspects of national security, defence, socio-economic stability and democratic order of the states affected, including on the cohesion of their respective societies.

The Cyber and Hybrid Threats Acquire Strategic Dimensions

Commerce, communications, individual privacy, intellectual property, and critical infrastructure, among others, all depend upon tools vulnerable to cyberattacks. Artificial intelligence (AI) compounds these concerns, remarks a Brookings study on reinvigorating multilateralism.[8] Consequently, the comprehensive embrace of cyber is much discussed. Dawn Thomas, an associate director and research analyst, argues that today cyber is much bigger than the "interconnected IT world." In her view, "cyber touches any part of society" (everything), and from that "everything" she identifies—and recommends to focus on—five areas in which cyberwarfare impacts society: Elections; Military secrets; Damage to infrastructure; Political and corporate espionage; and Polluting information spaces.[9] Cyberattacks by state and non-state "foreign actors," including state-sponsored actors, against democratic institutions, critical infrastructure and other governmental, military, economic, academic, social and corporate systems of both EU and NATO Member States have noticeably multiplied in the past few years, and have become more sophisticated, more destructive, more expensive and often indiscriminate. The US Identity Theft Resource Center revealed that the number of data breaches in the U.S. alone rose from 419 in

2010, with 23 million records stolen, to 1,579 in 2017, with the theft of 179 million records.[10]

Similar trends are observed on this side of the Atlantic, including in allied countries in Central and Eastern Europe. Bulgaria's National Centre on Information Security has reported "an abrupt increase" in the number of cyber incidents. In the first eight months of 2019 alone 2 028 531 incidents have been registered against 340 750 incidents in the same period of 2018. In comparison to 2017, this figure represents an increase of 20 times.[11]

Cyberattacks, including injections, can be particularly debilitating, with long-term and unpredictable negative consequences, when successfully implemented against electoral processes or disrupting the political and social fabric, including with a view to manipulating established public perceptions. Countries with functioning parliamentary democracy, rule of law and human rights standards—essentially EU and NATO Member States—are particularly vulnerable.

In a September 2016 letter to the FBI, the then Senate Minority Leader qualified the foreign attempts to cast doubt on free and fair elections as "a danger to democracy not seen since the Cold War."[12] A former U.S. Ambassador to Moscow interprets the Russian interference in the 2016 presidential elections as "an opportunity to take advantage of the polarization and dysfunction of the American political system" in order to "sow chaos and further dysfunction."[13]

The Ambassador's observation has been prophetically corroborated six months later by a USA Today/Suffolk University Poll which concluded that "Americans dread the 2020 election and have doubts about the outcome." The poll found "a sharply divided country" that views next year's presidential campaign as "a sobering test of the fundamental values of the United States." If the candidate they support loses, the poll finds, nearly four in 10 said they would have little or no confidence that the election had been conducted in a fair-and-square way, setting up what could be a debate over the legitimacy of the next president. Those expressing doubts crossed partisan lines – this view was shared by 30 % of the Republicans and 45 % of the Democrats.[14]

For the world's leading military power the reference to a "sharply divided country" should be taken as a serious warning at a time when Washington is forced to change its military strategy to one that would embrace a "competitive mobilization" capable of proving "decisive in a future great power conflict."[15] The divisions and the doubts expressed by respondents in the USA Today/Suffolk University Poll are probably due to a multiplicity of factors but targeted foreign influence operations at a time of national elections play a major role. By all means, Russia's actions prior and during the 2016 US presidential campaign will weigh heavily on the United States' national pride and self-confidence for a long time to come, and has already burdened the U.S.-Russia bilateral relations.

The resolve to establish the facts has been bi-partisan all along. From 2017 to 2019, the Select Committee on Intelligence of the U.S. Senate held hearings, conducted interviews, and reviewed intelligence related to Russian attempts in 2016 to access U.S. election infrastructure, and published a detailed report of five parts. The report's findings establish that the "Russian government directed extensive activity, beginning in at least 2014 and carrying into at least 2017, against U.S. election infrastructure at the state and local level," but also that "the Committee has seen no evidence that any votes were changed or that any voting machines were manipulated." The report admits further on that Russian intentions regarding U.S. election infrastructure "remain unclear." However, the Intelligence Committee (IC), based on what it knows about Russia's operating procedures and intentions more broadly, "assesses that Russia's activities against U.S. election infrastructure likely sought to further their overarching goal: undermining the integrity of elections and American confidence in democracy." A senior Homeland Security advisor testified in addition that "there was agreement in the IC that one of the motives that Russia was trying to do with this active measures campaign was to sow distrust and discord and lack of confidence in the voting process and the democratic process."[16]

On at least two public occasions President Trump said he believed the Russian leader's denials of Russian interference in the 2016 U.S. presidential election. Nonetheless, the key bipartisan finding of the fifth and final report of the Senate Intelligence Committee found that "the Russian government engaged in an aggressive, multi-faceted effort to influence the outcome of the 2016 presidential election."[17] The Senate Intelligence Committee's investigation into the massive intervention campaign waged by Russian government agencies and operatives on behalf of then-candidate Donald Trump was thorough, totalling more than three years of investigative activity, more than 200 witness interviews, and more than a million pages of reviewed documents. The investigation notes that unlike Mueller's report, which focused on questions of criminal conduct, the committee's report … is hundreds of pages of facts the panel obtained, drawing conclusions in places where Mueller often stopped short of doing.

In a similar reaction, the EU External Action Service has observed that "disinformation produced and/or spread by Russian sources has been reported in the context of several elections and referenda in the EU," too.[18]

At the 2020 Munich security conference Mark Zuckerberg, Facebook's founder, admitted that his company had been slow to understand Russian disinformation campaigns during the 2016 US election, as he appealed to political leaders for more regulation of online content.[19]

The EU has qualified the intentional generation and spread of disinformation by foreign actors as a "strategic challenge." While some experts do not consider "unleashing bots and trolls to push one's narrative" a cyberattack in the traditional definition, this type of foreign intrusion and intended destabilization can have both immediate and long-term consequences for Allied and EU-wide security and defence, and other strategic areas.

A cyberattack on the German parliament in 2015 (by "cyber programme" Sofacy/APT 28, believed to have close links with the Russian state) "sought to install software that would have given the hackers permanent access to computers used by staff and MPs." Other cyberattacks on Germany involved "gathering data about critical infrastructure." The attacks on German state organisations and institutions "were carried out to collect intelligence data," said the head of

Germany's domestic intelligence agency, BfV, and concluded that "cyberspace is a place of hybrid warfare, it opens up new operating areas for espionage and sabotage."[20] Shortly before he left office, former US National Security Advisor H.M. McMaster called the phenomenon of state-sponsored cyber-attacks a "sophisticated form of intelligence."

According to antivirus software company McAfee and the Center for Strategic and International Studies, the FBI and internet service providers have observed during 2017 a daily average of 80 billion malicious scans; 300,000 new pieces of malware; 33,000 phishing activities; and 4,000 ransomwares.[21] F. Lemieux further notes that the consequences of data breaches and cyberattacks can be costly in two ways: financial and reputational. For 2017, the financial cost of cybercrimes was estimated at between $500 billion and $600 billion worldwide. In terms of reputational impact, the professor quotes a study by Ponemon Institute, showing that organizations that suffered a data breach have experienced a 5 percent drop in average stock price the day a breach was announced and a 7 percent loss of customers.

The year 2017 saw a major shift in the direction of cyberattacks, cyber-theft and cyber-espionage towards economic and business targets in the U.S. and other OECD countries. Cyberspace remains a preferred operational domain for a wide range of industrial espionage threat actors – from adversarial nation states, to commercial enterprises operating under state influence, to sponsored activities conducted by proxy hacker groups, notes the US National Counterintelligence and Security Center in a 2018 report.[22] The report considers cyber economic espionage a "strategic threat" and points out that "China, Russia, and Iran (in this order) stand out as three of the most capable and active cyber actors tied to economic espionage and the potential theft of U.S. trade secrets and proprietary information." The areas of "the highest interest" have been identified as energy, including alternative energy; biotechnology; defence technology; environmental protection technology; high-end manufacturing; information and communication technology. To get an idea of the magnitude of the challenge, it is sufficient to give an example with just one targeted field: Information and Communication Technology (ICT). It involves eleven sectors, among them artificial intelligence (AI), big data analysis, core electronic industries, foundational software products, high-end computer chips, Internet of Things (IoT), network equipment, next-generation broadband wireless communications networks, and quantum computing and communications.

Analysing the economic, industrial and research areas of interest to foreign cyber-enabled economic espionage reveals that attempts to illegally acquire technology, industrial innovations and proprietary information are clearly geared towards technologies, processes and industrial samples conducive to gaining superiority in Industry 4.0 developments and in the emerging arms race on Earth and in Space.

To the extent that current trends in hacking patterns can be established, a report for 2019 indicates an increase in the number of nation-states acquiring offensive cyber capabilities from – the-shelf, as it were, and another report observes a sophistication of the threat landscape, allowing for identification of targeted, more in-depth, exploitation of personal data taken from massive data banks that have already been collected.[23] The last threat is judged to approximate a ticking time-bomb.

So far as the U.S. is concerned, challenges to its security and economic interests, from nation states and other groups, "which have long existed in the offline world are now increasingly occurring in cyberspace." In Washington's view, "this now-persistent engagement in cyberspace is already altering the strategic balance of power."[24]

Public Disclosure and Attribution of Cyberattacks and Hybrid Campaigns Make Good Deterrence Policy

Many of the attacks described above have had a disruptive effect but few of them, in particular in Europe, have been publicly reported, sometimes intentionally, with a view to preserving the civility of international dialogue or not to aggravate bilateral relations. Instantaneous, reticent denials by alleged perpetrator-states and a prevailing popular belief in non-professional circles that it is impossible to attribute an attack to a specific hacking entity or a person have also contributed to predominantly subdued reactions to foreign cyber intrusions, at least until recently.

A strong driver of change was the decision to let the U.S. intelligence and law enforcement agencies release public information on Russia's meddling, through cyber and non-cyber means, in the 2016 presidential elections. The revelations trend started at the end of the Obama administration and, regardless of occasional political considerations to suppress public disclosures, continues to this day.

Since 2010, at least half of the member states of NATO and of the EU, as well as several partner nations, have come on record to reveal publicly—with "a high degree of certainty" or based on formal court rulings and/or statements by law enforcement authorities—the origin and other relevant data of specific state-sponsored cyberattacks. On two notable recent occasions the individual perpetrators have been officially identified and taken measures against. In the first instance, the U.S. Justice Department charged seven Russian citizens with hacking officials investigating the Olympics doping scandal and the Skripal poisoning case, and with launching a cyberattack on a US power station.[25] In the second case, a Netherlands-UK joint counterintelligence operation was reported to have led to the arrest and expulsion of four Russian military intelligence officers in April 2018 for attempting to hack the Organization for the Prohibition of Chemical Weapons (OPCW).[26] The French Ministry of Foreign Affairs expressed "full solidarity" with the UK and the Netherlands on the role of Russia in the attack against the Organization for the Prohibition of Chemical Weapons (OPCW). It also noted that "the international law applies to cyberspace as well and France expects other countries to comply with it."[27]

To date, probably the most explicit and technically detailed public warning in regard to state-sponsored malicious cyber activities is the joint Technical Alert

(TA) of April 2018, issued by the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the United Kingdom's National Cyber Security Centre (NCSC). The Technical Alert provides information on "the worldwide cyber exploitation of network infrastructure devices (e.g., router, switch, firewall, Network-based Intrusion Detection System (NIDS) devices) by Russian state-sponsored cyber actors." It further reveals that "targets are primarily government and private-sector organizations, critical infrastructure providers, and the Internet service providers (ISPs) supporting these sectors." The specificity of the technical information provided in the TA "on the tactics, techniques, and procedures (TTPs) used by Russian state-sponsored cyber actors to compromise victims" exceeds any previous public disclosures.[28]

The Technical Alert (TA) provides rich food for thought and prompts several preliminary conclusions. First, the scope of the cyber threat has reached global dimensions, commensurate with the increasing scope of Internet and related information and communication networks and devices. Second, the range of government and private sector targets of cyberattacks is practically unlimited, which places steep requirements to resilience strategies and other countermeasures, including the acquisition of offensive capabilities by allies and partners. Third, the technical information on tactics, techniques and procedures (TTPs) can have the necessary "lessons learnt" effect only if regularly updated, shared and analysed in allied and partner formats, as appropriate. Fourth, the TA is a convincing illustration of the irreplaceable role of multilateral cooperation among allies and partners in delivering common cybersecurity. The value and relevancy of the Technical Alert is due to, and is made possible through "a coordinated series of actions between U.S. and international partners," involving in particular "previous DHS reporting and advisories from the UK, Australia and the European Union." Fifth, in some cases, reliable identification of the magnitude of a cyberattack, its victims and perpetrators, can only be reached through multilateral coordination and, if necessary, over prolonged periods of time. As demonstrated by other sources, it takes time for the applicable cyber "forensic" searches to be completed in order to establish with certainty the source and perpetrator of a cyberattack – through electronic evidence, sometimes tracing leaks and signals years back.

In this context, intelligence operations become ever more necessary, a point made by NATO Secretary General Jens Stoltenberg when announcing the establishment of a new NATO intelligence division. Its mission has been described by the Secretary General as coordinating "even better the way we collect, understand and analyse intelligence," including in connection with NATO establishing cyber as a distinct domain of operations.[29]

In the aforementioned Technical Alert, the FBI, in a separate individual move, has expressed "high confidence" that Russian state-sponsored cyber actors are using compromised routers "to conduct man-in-the-middle attacks to support espionage, extract intellectual property, maintain persistent access to victim networks, and potentially lay a foundation for future offensive operations."[30] This assessment of the potential impact of a directed series of cyberattacks presents the cyber threat not just as a technical problem but rather as a complex security and defence challenge – a foreign adversarial operation that can be exploited, by either human or artificial intelligence, to generate negative consequences for the security, including economic security, defence, law enforcement, critical infrastructure and other key interests of an affected state.

This brings us to the crux of the matter: could some of the adversarial cyberattacks and malicious cyber intrusions already be considered a clearly defined security breach—in contravention of international law—and what should a proportionate response entail? The views on this question of both NATO and the EU, and individual nations, have evolved in recent years. Presently, they increasingly tend to regard a cyberattack on vital or critical assets, including in cases in which it is a stage or a part of a wider hybrid campaign, as a systemic security challenge, which demands appropriate and adequate counter measures, both cyber and non-cyber.

NATO in particular has agreed on a response sequence, employing a combination of national capabilities, on a voluntary basis, and the full implementation of "the Cyber Defence Pledge, which is central to enhancing cyber resilience and raising the costs of a cyberattack." The Allies expressed determination, reaffirming NATO's defensive mandate, "to employ the full range of capabilities, including cyber, to deter, defend against, and to counter the full spectrum of cyber threats, including those conducted as part of a hybrid campaign."[31] The Allies pledge "to work together to develop measures which would enable us to impose costs on those who harm us". Individual Allies may consider, when appropriate, attributing malicious cyber activity and responding in a coordinated manner, recognising that attribution is a sovereign national prerogative. The "imposing costs" option is further elaborated and strengthened in the U.S. Cyber Strategy.

Publicly attributing malicious cyber activity is becoming the norm rather than an exception. In the absence of an international body which would deal with complaints of foreign cyberattacks, affected democratic states most often prefer to go public about having sustained a cyberattack or a disinformation and/or hybrid campaign. Increasingly, governments believe that the public at large—citizens, civic organisations, businesses, academia as well as the international community—should be openly informed about foreign cyberattacks and their implications, as well as, in certain cases, on any deterrence and defence measures undertaken. A transparent and robust cybersecurity stance or revelation can deprive the perpetrators of the "silence" and "invisibility" effects of a cyberattack/intrusion, increase the level of resilience to cyber hacks and hybrid campaigns, and lay the legal ground for not only holding the implicated state or a state-sponsored entity accountable for the attack(s) but also, for taking (offensive) counter measures.

Still, a number of authors believe that attribution remains a problem in cyberspace for one main reason: attribution is inherently uncertain as suspected states will always have sufficient deniability, whether it is because of false flag attacks, or by putting a distance between them and the attackers. This inherent uncertainty makes proportional retaliation harder for targeted states, as it will entail a judgement call.[32]

The Nexus between Cyberattacks and Hybrid Operations

Cyberattacks range from waging massive phishing campaigns to stealing business secrets, sensitive technology and proprietary information, and to critical infrastructure penetration and manipulation. In the past six months the EU has openly stigmatized both Russia and China for misinformation campaigns concerning the COVID-19 pandemic and for attempts to interfere with and hack vaccine research and production. Hacking and other forms of cyberattacks and cyber warfare are however rarely an end in themselves: in many cases they represent a stage in wider hybrid campaigns, seeking disinformation or disruptive effects, including supporting spying operations.

Recent election-related hacking, combined with specific information tampering and subversive operations and other hybrid designs, represents a new systemic threat against the core pillars of democracy. Democratic societies have reacted angrily, indicating they are not prepared to live with digital gerrymandering or other forms of sophisticated cyber social engineering capable of eroding the substance and independence of the democratic electoral process.

In its April 2016 Joint Framework on Countering Hybrid Threats the EU notes that, while definitions of hybrid threats vary and "need to remain flexible to respond to their evolving nature," the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare.[33]

Based on observations of foreign armed forces' behaviour across the military domain, the outgoing chairman of the Joint Chief of Staff Marine Corps Gen. Joe Dunford emphasised the same point, stating that "our adversarial competitors" favour strategies that go right up to the edge of conflict but do not cross the threshold.[34] Covert cooperation between government institutions and "private" or "patriotic-minded" hackers for planning and carrying out cyberattacks against a foreign state additionally blurs the perpetrators' identity and complicates the initiation of counter measures by the affected party. In this connection a BBC security correspondent recently wrote: "…as the field that is newest, the rules in cyber-space of what constitutes war and an attack are much less clear. And that may be the danger, as miscalculation could lead to escalation."[35]

Cyber Warfare in Combat Conditions

While both NATO and the EU have taken an integrated or a holistic approach to cyber- and hybrid attacks, meaning—in broad terms—developing measures to prevent and deter adversarial cyberattacks and intrusions onto both "civilian" and "military" targets, there are specific cyberattacks that concern strictly the Allies' military domain, including combat training. This article only addresses military domain-related cyberattacks in principle and in limited terms.

Cyber warfare, when undertaken in combat conditions, would be a qualitatively different and much graver challenge to international peace and stability, reflecting the changing character of modern conflict and the military and technological drivers of this change. Missions in cyberspace will be an integral part of military operations. Modern warfare is changing fast and in profound ways, influenced by developments in the fields of artificial intelligence (AI), directed-energy weapons, hypersonic technologies and other innovations, which, among others, require exceptionally quick decision-making – in some cases striving for direct "data to decision" solutions.[36]

Cyberspace is expected to be a new factor in, for example, calculations on, and perceptions of, anti-access/area denial (A2/AD) capabilities, which are crucial to NATO doctrine of defence and deterrence. For example, says London-based International Institute for Strategic Studies, a combatant could deny an adversary access to any area of operation by crippling their home logistics and support infrastructure, thereby sabotaging through cyber means their ability to project military power.[37]

Today cyberspace is rapidly becoming "a crucial and contested war-fighting domain in its own right." NATO regards hostile hybrid operations as demanding the highest level of military and political response, believing that it is the hybrid activities that "aim to create ambiguity and blur the lines between peace, crisis, and conflict." Accordingly, NATO has reaffirmed and is strengthening its resolve, first declared in 2016, under certain circumstances and in cases of hybrid warfare against an Ally, to initiate a procedure under which the Council could decide to invoke Article 5 of the Washington Treaty, "as in the case of armed attack."[38]

Scope of the Cyber Threat

With the cyber threat having such a diverse and destabilizing nature, as discussed above, the question arises as to what exactly should be considered "cyberspace." The latter's identification and description would facilitate the methodological task of specifying the scope of the cyber threat and, respectively, the political, technical and legal aspects of an affected state's or an Alliance-authorised response.

The U.S. National Counterintelligence and Security Center defines Cyberspace as "(a) the interdependent network of information technology infrastructures; and (b) including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[39] This comprehensive definition gives a realistic idea of the immense array of users, assets and systems that can potentially fall under cyberattacks (thus suggesting a need for an in-depth study of the problem in a separate article).

The particular issue of embedded processors and controllers, as an element of the definition of cyberspace, is addressed here by way of an illustrative example. Industry experts point out that 98 % of all microprocessors are manufactured components of embedded systems. These systems are found in consumer, industrial, automotive, medical, commercial and military applications as well as in transportation, fire safety, security, and life critical systems, and the list is not complete. In principle, the embedded systems can be made more reliable and isolated from hacking when they are not connected to wired or wireless networks.

The vulnerabilities of Internet-connected devices are relevant, among others, to Internet of Things (IoT), the fast-growing network of billions of physical objects and sensors being used to transmit data and automate basic functions. The problem is that ever more users reportedly prefer or simply rely on IoT devices to transmit sensitive, mission-critical information (including military or strategic in nature) from remote locations around the world or from places far from the "core," thus creating a hitherto overlooked cybersecurity issue "at the edge." A recent study has revealed that the higher-grades employees of up to 30 U.S. federal departments and agencies, including Defence, Joint Chiefs of Staff, State, Home Security, Energy, Commerce and Transportation, extensively use Internet-powered devices whose standard encryption and automation protocols do not necessarily protect against cyberattacks, causing experts to propose a federal-wide system of IoT cyber protection.[40] One can only imagine the magnitude of the problem to be created by IoT devices possibly used for "official" purposes across all Allied networks of communication.

The vulnerability of IoT chain of devices (and any other connected equipment for that matter) is further exacerbated by much discussed in-built "back doors" in certain communication brands (Huawei), in particular when connected to 5G networks (and subjected to foreign national legislation obliging companies to collect clandestinely). Washington is concerned that Allies who insist on using equipment of these brands will have to be excluded from intelligence sharing arrangements. EU's approach, still in the making, seems to be more accommodating to controversial equipment. Basically, it relies on "measures and regulations rather than bans": the European Commission…recommended that the bloc, after having assessed the risks, immediately take measures to protect their 5G networks. In particular, these measures should include reinforced obligations on suppliers and operators to ensure the security of sensitive parts of the networks.[41]

On the other hand, software developers in the U.S. seem to have a solution to the 5G Huawei dilemma. The 5G standard itself is open and interoperable; the RAN (radio access network) is described as software that takes in radio signals and digitizes them, or vice versa. Because such functionality is complex, intensive, and happens in real time—observes Tom Wheeler, Visiting Fellow at the Centre for Technology Innovation—the infrastructure companies, "have each developed their own approach that conveniently locks in the purchaser: the open and interoperable 5G standard has thus become buried behind closed proprietary infrastructure."[42] The way then is in adopting practices that make 5G open like most of the rest of the digital world: accordingly, one needs to replace traditional network vendors' proprietary technology with software-driven technology that will run on any off-the-shelf hardware.

To sum up, the disruptive cyber threat covers potentially all critical systems of a nation-state in the civilian and defence domains, including related Allied and EU assets, albeit not necessarily in simultaneous attacks and not coming from a single source. Artificial intelligence (AI) and machine-learning (ML) will make the cyber threat scalable and perhaps even autonomous, further enlarging the operational scope of the cyber threat and the attack surface that hackers can target.

The AI Dimension of the Cyber Threat

While some AI algorithms and methodologies have already been used "maliciously" on the Internet, scientists warn that we are witnessing a "co-evolution" of Artificial Intelligence (AI), Machine Learning (ML) and cybersecurity, the cumulative effect of which amounts to "a game-changer." The same phenomenon is fuelling "a profound military revolution." The common threat denominator of these new developments is the autonomous nature of AI and ML programmes and applications, which is a distinct and potentially disruptive feature of these technologies. The expectation that humans may therefore no longer remain "in the loop" seems increasingly plausible, a prospect which, if allowed to take place, in particular in the military domain, could lead to catastrophic scenarios. For example, a [Chinese] development team working on creating "AI with own thinking," managing to design "a runaway submarine with enough nuclear arsenals to destroy a continent."[43]

In the event of attacks by autonomous weapon systems, the level of anonymity and the negligent "psychological distance," compared to the one between a "traditional" operator and a push button, lower the threshold for use of military force. The same factors also make it more difficult to attribute an assault.

The international debate on AI and ML in the context of Industry 4.0, quantum science and quantum computing, among others, has been going on for a number of years now but only recently has this debate touched on the interrelationship between AI, ML and the cyber threat. A report, entitled "The Malicious Use of Artificial Intelligence"—the product of twenty eight authors coming from over 20 research institutions and think-tanks—provides a broad and realistic picture of the sorts of attacks we are likely to see soon if adequate responses are not developed.[44] The co-evolution of "classic" cyber threats and artificial intelligence (AI) and machine learning (ML), put to work together, introduces further destabilizing trends in warfare, states the report, and alters the landscape of security risks for citizens, organizations, businesses and states. With a view to covering all potential cyber threats, the report suggests to designate three main areas of cybersecurity: digital security – the threats coming from training machines to hack or socially engineer victims "at superhuman performance", e.g. mass spear phishing; physical security – an example has been given with "non-state actors weaponizing consumer drones"; and political security – countering insidious attacks such as privacy-eliminating surveillance, profiling, repression, and automated disinformation campaigns.

The current research on quantum computing is another looming threat to digital cryptography, with implications for national security, including confidential corporate and state data as well as sensitive personal information, finds a report by the US National Academy of Sciences, Engineering and Medicine, sponsored by the Office of Director of National Intelligence. The report recommends that new cryptography must be developed and deployed now, even if quantum threats are a decade away.[45] The 2019 pre-Davos conference report warns that the collapse of cryptography would take with it much of the scaffolding of digital life: these technologies are at the root of online authentication, trust and even personal identity, and they keep fundamental services running. What is more, even if a transition to new alternatives (i.e. lattice-based cryptography) takes place soon, or if sensitive information is managed offline only, stored, conventionally encrypted data will be vulnerable once quantum advances allow accessing it.[46] Thus, "invisible" cyber theft could, with time, prove to be materially detrimental to the security, defence and social stability of a NATO or an EU member state, or several of them.

Building a Coherent Response Strategy to Cyber and Hybrid Threats

The principles of NATO's response strategy have been agreed by the Allies, albeit in rather broad terms. NATO will have to complete the process of designing and building Allied cyber systems securely, and develop doctrine and policy on sharing critical cyber intelligence in real time and on integrating national cyber capabilities. According to plan, the Alliance has another 2 to 3 years to set up the Cyber Security Centre in Mons, Belgium, and to select the 70 top experts needed to operate it. When this work is completed, it is expected that the Alliance will be in a position to integrate and coordinate the activities of its member states.

The core of the response strategy should be the development of adequate national cyber capabilities, including offensive ones, as well as allied procedures and platforms for exchange of information and intelligence, joint cyber training, coordinating cyber and non-cyber means, and raising public awareness campaigns – with a view to creating a shield, as comprehensive as possible, against all sorts of cyberattacks, including related hybrid campaigns and misinformation operations. The latter adversarial activity has been gaining ground in the past few years while the necessary counteraction is only now beginning to take shape with the (delayed) involvement of social media- and global tech companies, which are uniquely placed to contribute to finding lasting solutions.

The EU in its own right seems ready to go as far as imposing sanctions in instances of state-sponsored cyber-based hybrid attacks. However, very much like NATO declaring readiness but having not yet agreed on procedures for enacting Article 5 when confronted with a major cyberattack and/or a hybrid campaign, the EU has not elaborated sufficiently on the modalities of making its sanctions operational.

In July 2020, the German government has said the EU should impose sanctions on Russian hackers responsible for the cyberattack on the Bundestag in 2015. If agreed, wrote EU Observer, this could be the first use of the EU cyber sanctions scheme adopted in 2017. Some 16 gigabytes of data, documents, and emails were stolen from the Bundestag's network, including thousands of emails from Angela Merkel's office.[47]

An important part of the strategy will have to be resilience building and risk-reduction activities. Measures should cover, as a minimum, several key areas such as the national security and defence system; energy and power; banking and finance; health and safety; communications; information technology; and transportation. These areas seem to command agreement and enjoy support by NATO and EU member states alike.

With all reservations and slight differences in doctrine between some member states, it can be safely concluded that both NATO and the EU, including through direct and closer cooperation between the two blocs, will be able to enhance the resilience of their societies to cyber and hybrid threats, and to develop adequate national cyber capabilities. This is a process in development: closer national governments' support and scrutiny, and innovative thinking, are much needed. Several Allies, notably the UK, U.S., Germany, France, Estonia, the Netherlands, etc. have gained valuable experience in cyber security and cyber defence matters and have advanced considerably in the capability of assessing and operationalizing the cyber threat and response techniques, including offensive capabilities. For some of them, their unique expertise relies on "intelligence knowledge" based on "real, hard facts about what the adversary is trying to do." Establishing an in-depth and reliable Allied information and intelligence sharing mechanism is of paramount importance.

The United States should be encouraged to play a major role, given its military, scientific, technological, commercial and strategic interests related to cybersecurity as well as its exceptional potential to contribute to the common goal. It is noteworthy that regardless of a nationalist and isolationist tendency in American policy, the U.S. will most likely intensify cooperation and coordination with Allies and Partners in all aspects of the cyber domain: a review of the targets and outcomes envisaged under all the eight "pillars" in the U.S. National Cyber Strategy clearly shows that the U.S. relies heavily on allied cooperation. The Cyber Strategy is shy of mentioning the EU expressly but when it comes to practical work, EU-US cooperation, dating back to 2010, has proven useful to both sides.

The 2019 U.S. cyberattack, targeting missile command and control systems of the Iranian Islamic Revolutionary Guard Corps, in retaliation for Iran's physical attack on a U.S. military drone, is an indication of a major shift in Washington's cyberwar strategy. In particular, this first "publicly acknowledged" attack implies that the U.S. Cyber Strategy has, within a relatively short period of time, led to the elaboration of new guidelines, streamlining and considerably shortening the approval process for conducting cyberattacks on U.S. adversaries (the "button" was pushed only hours after the U.S. drone was shot down). A critical element of the decision to initiate a crippling cyberattack was a humanitarian consideration – in American estimates, a "traditional" military strike would have led to civilian casualties.[48] This consideration of the American cyber assault has perhaps cushioned the Iranian and the international reactions but in-depth analyses on the tactical and strategic repercussions of this first cyber strike of its kind will not be long in coming.

The U.S. offensive cyberattack is a reflection of a growing conviction that the classical concept of strategic deterrence has its limitations in cyberspace. Yet, analysts with experience in nuclear disarmament and arms control negotiations believe that by starting with simple principles of tackling the problem—for example, negotiating a mixture of formal and informal mechanisms; and pursuing focused and single-issue rather than broad and general agreements—the international community can initiate a process of "cyber arms control."[49]

Today, great power confrontation, asymmetry in the evolving strategic situation, openly expansionist foreign and security policy designs by adversaries such as the ones mentioned in this article create a complex and volatile international setting. It is unlikely that any of these adversaries, including non-state actors with their own anti-Western agendas, will in earnest be willing to forego recourse and use of such an effective and "cheap" weapon as cyber malicious capabilities. Both the EU and NATO cannot and should not however give up on their long-term strategies to prevent unpredictable and disruptive behaviour in the cyberspace. Due to the nature of cyberspace, working jointly on addressing the cyber and hybrid threat by Allies on both sides of the Atlantic will have a beneficial effect on Alliance unity and solidarity and on EU-NATO cooperation – a prerequisite for a successful engagement with the rest of the world on regulating cyberspace.

References

[1] *National Cyber Strategy of the United States of America* (Washington, D.C.: The White House, September 2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[2] NATO, "Brussels Summit Declaration," 11-12 July 2018, Para. 20, www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_11/20181105_1811-factsheet-key-decisions-su.pdf.

[3] Human Factors & Medicine Panel, NATO Science & Technology Organization, HFM-288, Research Workshop on "Integrated Approach to Cyber Defence: Human in the Loop," Sofia, Bulgaria, 16-18 April 2018. Selected papers presented at the workshop were published in Yantsislav Yanakiev, *Integrated Approach to Cyber Defence: Human in the Loop*, *Information & Security: An International Journal* 45 (2020), https://doi.org/10.11610/isij.v44.

[4] Sabi I. Sabev, "Integrated Approach to Cyber Defence: Human in the Loop. Technical Evaluation Report," *Information & Security: An International Journal* 44 (2020): 76-92, https://doi.org/10.11610/isij.4407.

[5] Peter Poptchev, "The Importance of Doctrinal Alignment and Structured Coordination among NATO and EU Member States for Developing a Holistic Cybersecurity and Cyber Defence Strategy," NATO Science & Technology Organization, Research Workshop on Integrated Approach to Cyber Defence: Human in the Loop, Sofia, Bulgaria, 16-18 April 2018.

[6] Robin Emmott, "NATO Cyber Command to Be Fully Operational in 2023," *Reuters*, October 16, 2018.

[7] Jens Stoltenberg, "Meeting the Press," *NATO Newsroom*, October 5, 2018.

[8] Bruce Jones, Jeffrey Feltman, and Will Moreland, "Competitive Multilateralism: Adapting Institutions to Meet the New Geopolitical Environment," The Brookings Institution, September 2019, https://www.brookings.edu/wp-content/uploads/2019/09/FP_20190918_competitive_multilateralism_FINAL.pdf.

[9] "Ep. 48: Cyberwarfare today," Defense One Radio, Washington D.C., July 12, 2019, https://www.defenseone.com/ideas/2019/07/ep-48-cyberwarfare-today/158387/.

[10] Frederic Lemieux, "How to Tackle Cybersecurity Risks More Effectively," Georgetown University, School of Continuing Studies, September 17, 2018, https://scs.georgetown.edu/news-and-events/article/7329/how-tackle-cybersecurity-risks-more-effectively.

[11] "Brussels Dispatches an Expert Team to Check on the Cybersecurity in This Country," *Mediapool.bg*, September 10, 2019 (in Bulgarian).

[12] Mike Levine and Pierre Thomas, "Russian Hackers Targeted Nearly Half of States' Voter Registration Systems, Successfully Infiltrated 4," *ABC News*, September 29, 2016, https://abcnews.go.com/US/russian-hackers-targeted-half-states-voter-registration-systems/story?id=42435822.

[13] James Fallows, "'Chaos Serves Putin's Interest': A Veteran Diplomat Takes Stock," an interview with William J. Burns, *The Atlantic*, March 11, 2019, https://www.defenseone.com/ideas/2019/03/bill-burns-chaos-serves-putins-interest/155440/.

[14] Susan Page, Jason Lalljee, and Jeanine Santucci, "Who's Gonna Make the Debate Stage?" *POLITICO*, 28 August, 2019, https://www.politico.com/newsletters/playbook/2019/08/28/whos-gonna-make-the-debate-stage-473330.

[15] Elsa Kania and Emma More, "The US is Unprepared to Mobilize for Great Power Conflict," *Defense One*, July 21, 2019, https://www.defenseone.com/ideas/2019/07/us-unprepared-mobilize-great-power-conflict/158560/.

[16] "Report of the Select Committee on Intelligence," United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 1: Russian Efforts against Election Infrastructure with Additional Views, Section V: Russian Intentions, 2016, p. 35.

[17] "'We Must Do Better in 2020': Bipartisan Senate Panel Releases Final Report on Russian 2016 Election Interference," *Homeland Security News Wire*, August 18, 2020, http://www.homelandsecuritynewswire.com/we-must-do-better-2020-bipartisan-senate-panel-releases-final-report-russian-2016-election-interfere.

[18] European Commission, "Action Plan against Disinformation," High Representative of the Union for Foreign Affairs and Security Policy, Brussels, JOIN (2018) 36 final, December 05, 2018, p. 4., https://ec.europa.eu/commission/publications/action-plan-disinformation-commission-contribution-european-council-13-14-december-2018_en.

[19] Helen Warrell, Guy Chazan, and Michael Peel, "Mark Zuckerberg Admits Facebook Was Slow on Russian Disinformation," *Financial Times*, February 15, 2020, www-ft-com.eur.idm.oclc.org/content/5b42ef72-501e-11ea-8841-482eed0038b1.

[20] "Russia 'was behind German parliamentary hack'," *BBC News*, 13 May 2016, https://www.bbc.com/news/technology-36284447.

[21] Lemieux, "How to Tackle Cybersecurity Risks More Effectively."

[22] US NCSC, "Foreign Economic Espionage in Cyberspace," National Counterintelligence and Security Center, 2018, https://www.dni.gov/files/NCSC/documents/news/2018 0724-economic-espionage-pub.pdf.

[23] "Ep.48: Cyberwarfare today."

[24] *National Cyber Strategy of the United States of America*, Pillar III: Preserve Peace through Strength.

[25] Hannah Parry, "Justice Department Indicts Seven Russian Spies for Hacking Olympic Doping Scandal Investigators, Launching a Cyber Attack on a US Nuclear Company and for Trying to Undermine the Probe into ex-KGB Officer Poisoning in the UK," *Dailymail.com*, October 4, 2018, https://www.dailymail.co.uk/news/article-6240621/Russia-accused-cyberattacks-investigators-pursuing-doping-poisoning-cases.html.

[26] David Salvo and Bradley Hanlon, "Key Takeaways from the Kremlin's Recent Interference Offensive," *Homeland Security News Wire*, 11 October 2018, http://www.home landsecuritynewswire.com/dr20181011-key-takeaways-from-the-kremlin-s-recent-interference-offensive.

[27] France-Press, TASS, and Bulgarian Telegraph Agency, as quoted by *Mediapool.bg*, 5 October 2018.

[28] "Joint US - UK Statement on Malicious Cyber Activity Carried out by Russian Government," National Cyber Security Centre, April 15, 2018, www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government.

[29] "Press conference by NATO Secretary General Jens Stoltenberg following the meetings of NATO Defence Ministers," Brussels, 04 October 2018.

[30] US Department of Homeland Security, "Alert (TA18-106A) Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices," April 20, 2018, https://us-cert.cisa.gov/ncas/alerts/TA18-106A.

[31] NATO, "Brussels Summit Declaration," Para. 21.

[32] Eva-Nour Repussard, "There Is No Attribution Problem, Only a Diplomatic One," *King's College University*, December 2019, https://www.e-ir.info/2020/03/22/there-is-no-attribution-problem-only-a-diplomatic-one/.

[33] "Joint Framework on Countering Hybrid Threats," JOIN (2016) 18 final, High Representative of the Union for Foreign Affairs and Security Policy, Brussels, April 6, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.

[34] Jim Garamone, "Dunford: Global Security Environment Has Implications for Joint Force," *DoD News*, November 29, 2016, https://www.defense.gov/Explore/News/Article/Article/1017146/dunford-global-security-environment-has-implications-for-joint-force/.

[35] Gordon Corera, "Could Russia and West be Heading for Cyber-war?" *BBC News*, October 4, 2018, https://www.bbc.com/news/technology-43788114.

[36] Todor Tagarev, Raphael Perl, and Valeri Ratchev, "Recommendations and Courses of Action: How to Secure the Post-Covid Future," in *Transatlantic Security: Securing the Post Covid Future*, edited by IBM (Wien: Federal Ministry of Defense, 2020), 18-41.

[37] *Strategic Survey 2016: The Annual Review of World Affairs* (London: IISS, 2016), 65.

[38] "Brussels Summit Declaration."

[39] US NCSC, "Foreign Economic Espionage in Cyberspace."

[40] "Securing the Edge: Surveying the Vulnerabilities in the Federal Government's Internet of Things," Research report, Government Business Council, Brocade Communications System, January 2017, https://www.cybersecobservatory.com/wp-content/uploads/2017/05/security-at-edge.pdf.

[41] Irene Kostaki, "EU Struggles to Balance Trans-Atlantic Ties with Exposure to Huawei," New Europe, Brussels, 31 March 2019.

[42] Tom Wheeler, "Moving from 'Secret Sauce' to Open Standards for 5G," *Brookings Global Eye*, February 18, 2020, https://globaleye.online/moving-from-secret-sauce-to-open-standards-for-5g-brookings/.

[43] Christina Zhao, "China Building Artificial Intelligence–Powered Nuclear Submarine That Could Have 'Its Own Thoughts,' Report Says," *Newsweek*, May 2, 2018, https://www.newsweek.com/china-building-artificial-intelligence-powered-nuclear-submarines-have-its-own-799351.

[44] Miles Brundage, Shahar Avin, Jack Clark, et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," Future of Humanity Institute – University of Oxford, Centre for the Study of Existential Risk, Center for a New American Security, Electronic Frontier Foundation, Open AI, February 2018, https://arxiv.org/abs/1802.07228.

[45] "New Cryptography Must Be Developed and Deployed Now," *Homeland Security News Wire*, December 5, 2018, https://www.nationalacademies.org/news/2018/12/new-cryptography-must-be-developed-and-deployed-now-even-though-a-quantum-computer-that-could-compromise-todays-cryptography-is-likely-at-least-a-decade-away-says-new-report.

[46] World Economic Forum, "The Global Risks Report 2019," January 15, 2019, p. 67, https://www.weforum.org/reports/the-global-risks-report-2019.

[47] "Berlin Wants First Use of EU Cyber Sanctions on Russia," *EU Observer*, 13 July 2020, https://euobserver.com/tickers/148923.

[48] Ellen Nakashima, "Trump Approved Cyber-strikes Against Iranian Computer Database Used to Plan Attacks on Oil Tankers," *Washington Post*, June 23, 2019, https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html.

[49] Andrew Futter, "What Does Cyber Arms Control Look Like? Four Principles for Managing Cyber Risk," *Policy Brief*, European Leadership Network, June 2020,

https://www.europeanleadershipnetwork.org/policy-brief/what-does-cyber-arms-control-look-like-four-principles-for-managing-cyber-risk/.

About the Author

Peter **Poptchev**, PhD, is a career diplomat, having held rank-and-file and Head of Mission posts in Lagos, Geneva (Disarmament), Brussels (NATO), Dublin and Vienna (OSCE, UN). In 2007 he was appointed Bulgaria’s first Ambassador-at-large for energy security and climate change, and National Coordinator for the EU Nabucco project. He has chaired many multilateral negotiating formats at UN, Conference on Disarmament, EU, NATO, OSCE, etc. The author of four books and numerous articles, Ambassador Poptchev continues to work on foreign and security policy issues as an independent consultant. He has recently established an international network to study and foster the European Green Deal.