RESEARCH AND ANALYSIS

Hybrid CoE Trend Report 6

APRIL 2021

The future of cyberspace and hybrid threats

HYBRID COE EXPERT POOL MEETING ON CYBER

Hybrid CoE

Hybrid CoE Trend Report 6

The future of cyberspace and hybrid threats

HYBRID COE EXPERT POOL MEETING ON CYBER

Hybrid CoE Trend Reports are an outcome of expert pool meetings on a given theme. They highlight the main trends of the theme, provide multiple perspectives on current challenges as well as academic discourse on the topic, and serve as background material for policymakers. They aim to distinguish between what really constitutes a threat, what appears to be a threat but is not necessarily one, and what has the potential to become one. Hybrid CoE's Research and Analysis engages expert pools on relevant themes in the landscape of hybrid threats.

The European Centre of Excellence for Countering Hybrid Threats tel. +358 400 253800 www.hybridcoe.fi

ISBN 978-952-7282-69-4
ISSN 2670-1804

April 2021

Hybrid CoE is an international hub for practitioners and experts, building participating states' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats, located in Helsinki, Finland.

Contents

Foreword

The European security environment is becoming increasingly complex in nature. In addition to the traditional military domain, security threats are trickling down to all aspects of social life as democratic states encounter threats from actors who are willing and more able than ever before to attack domains not perceived as belonging to the core field of security, using a creative combination of multiple tools to achieve their goals and push their strategic interests in unacceptable ways.

Analyzing emerging trends related to security and highlighting long-term undercurrents will help in understanding the changing security environment, and in being better prepared to respond to potential hybrid threats in the future. Being able to read trends makes it easier to place current events in context and to distinguish between what is a threat, what looks like a threat but is not necessarily one, and what has the potential to become a threat in the future.

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) operates expert pools to support its Participating States and the activities of the Centre's Communities of Interest. The expert pools work as a forum for exchanging information, building connections and gaining a comprehensive understanding of the trends under a specific theme. These trends are then linked through Hybrid CoE to potential hybrid threats. The expert pools are an ongoing process and provide content for the Centre's work.

Engaging with the expert pools and the related activity is in line with Hybrid CoE's founding memorandum of understanding, which states that Hybrid CoE is to act as a hub of expertise, to offer collective expertise and to encourage strategic dialogue. This activity should adopt a multidisciplinary and academic approach. Thus, the purpose of engaging with the expert pools is not to pursue a single truth, but rather to provide multiple perspectives on current challenges, to provide perspectives on the academic discourse on the topic, and to serve as a background for policymakers. The added value of this work is that it examines the subject from a hybrid-threat perspective. Each Participating State, the EU and NATO can then consider which facets of knowledge will be most useful from its own perspective.

This report is based on Hybrid CoE's Cyber Expert Pool's first meeting, which was held in Helsinki, Finland on 12–13 February 2020. The report was compiled by Dr Catharina Candolin, from the Defence Command Finland, based on the meeting outcomes and expert pool members' comments, together with Hybrid CoE Director of Research and Analysis Hanna Smith, Deputy Director of COI Strategy and Defence Josef Schröfl, and Coordinator Emma Lappalainen.

Introduction

Although the concepts pertaining to hybrid threats have received much criticism, they have proved to be very useful characterizations in relation to the changing security environment, and in rethinking security, solidarity and alliances in the 21st century. The characterization of an activity as a hybrid threat is based on identifying activities that – when deliberately combined and synchronized by an actor with malicious intent – pose a unique threat to the interests of the target state.

Cyber is but one of the **domains** in which hybrid threats occur.[1] It should be noted that hostile activity in the cyber domain alone does not constitute a hybrid threat, but becomes such when multiple tools, and vulnerabilities in other domains are simultaneously used by an actor in order to reach the same goal. Most hybrid threat activity comprises elements of both cyber and information operations.

There are underlying conditions that increase the prominence of the cyber domain in the framework of hybrid threats. First of all, **states base their development on the rapid advancement of technology**. While this has been beneficial for states on a multitude of levels, it has also made them vulnerable to threats in cyberspace. Second, **the capabilities of states and criminals to operate in cyberspace have developed**; some are highly advanced, while others are mainly persistent. Nevertheless, the number of successful cyberattacks has increased. Third, **cyberspace is the main enabler of the global dissemination of information**. However, this also includes disinformation and misinformation.

These three phenomena of the modern world increase prosperity and interconnectedness, and the vast opportunities are enjoyed by both big and small, friendly and hostile states, as well as criminals. States consider cyberspace fertile ground for information campaigns, whereas criminals utilize it for economic purposes for the most part. It is worth noting that most political and military conflicts now have a cyber dimension. This emphasizes the increasing importance of the cyber domain for unconventional hybrid threats, as it is particularly empowering for states that do not have the military capacity of larger powers. Cyber proficiency levels the playing field – or battleground – to a certain extent.

The main objective of this report is to discuss the development of cyberspace as an enabler of both cyber operations and cyber-enabled information operations, and to cover future developments of cyberspace and hybrid threats. The Hybrid CoE Cyber Expert Pool meeting identified three current trends of hybrid threats in the cyber domain: **an increase in the disruptive use of artificial intelligence; the expansion of the role of cyber during times of crisis;** and **growth in dependencies between policy and technology**. The three trends are examined from the point of view of relevant technological developments and the possibilities for cascading effects. Also of note is the fact that each of these trends has a cross-cutting information-operation element enabled by cyber. The chapters conclude with open questions that the reader can take into account when considering future developments of the cyber domain and hybrid threats.

1 According to the conceptual model developed by Hybrid CoE and the EC's Joint Research Centre, hybrid threats can be observed in 13 different domains: administration, culture, cyber, diplomacy, economy, information, infrastructure, intelligence, legal, military, political, social, and space. See Giannopoulos et al, 'The Landscape of Hybrid Threats: A conceptual model', 26–32.

TREND 1: Increase in the disruptive use of artificial intelligence

Artificial Intelligence (AI) is one of the main technology trends affecting the cyber domain at the present time. AI and machine learning are developing at a tremendous pace and an increasing number of applications utilize AI as a part of their solutions. At the moment, the use of AI is largely restricted to a specific task that is either routine or that requires the processing of a huge amount of data; tasks that human beings are not really qualified to do. Computers are more capable of performing repetitive tasks and are also able to process large quantities of data in a short space of time, all while learning. While advancements in AI are not as striking as imagined, the development has increased productivity and performance quality, improving decision-making capabilities, for example. However, this technology has its dark side as well: an actor that wants to inflict harm can find AI a useful instrument for malign – or disruptive – purposes.

The technological advancements in AI will have increasing implications for the cyber domain. Cyberattacks can become more cost-efficient as AI is incorporated into tasks currently performed by people. This will enable a growing number of actors to carry out attacks at an increasing speed, towards an increasing number of targets. Furthermore, new threats will emerge as AI solutions can accomplish tasks that are too complex for human beings, for example, exploiting the vulnerabilities of the defenders' AI systems. Offensive cyber operations supported by AI solutions will be highly efficient, precisely targeted, and difficult to attribute.

In the near future, some of the main AI-supported cyber threats might be produced by using automated hacking, speech synthesis used to impersonate targets, finely-targeted spam emails using information scraped from social media, or by exploiting the vulnerabilities of AI systems themselves (e.g. through adversarial examples and data poisoning).[2]

Increasing surprises and cascading effects from the cyber-physical domain

An increasing number of operations in the physical domain are dependent upon the cyber domain. This has given rise to the concept of the "cyber-physical domain".

When it comes to the cyber-physical domain, critical infrastructure is particularly relevant. For example, in logistics and transportation, land (road and rail), sea, and air traffic control is reliant upon digital systems in several ways. The disruption to, or destruction of, critical infrastructure (systems, plants, processes, networks, and devices) would have a serious impact on the health, safety, economic and social wellbeing of the population, as well as the functioning of governance structures. Critical infrastructure includes, but is not limited to, energy production and distribution (e.g. the electrical grid, heating), communication systems, transportation and logistics, healthcare, and water supplies.

Many infrastructures such as the energy infrastructure rely on autonomous systems. The healthcare system relies on the availability of information systems to ensure that patient data, for example, can be collected from the necessary sources and used when and where needed, sometimes even in emergency situations. Critical infrastructure and fundamental functions and services are interconnected.

In addition to the benefits of increased efficiency and effectiveness, the dependencies give

2 Roberts, 'Global AI experts sound the alarm'; Hybrid CoE expert-pool discussion 2020.

rise to new types of vulnerabilities. Advances in automation engender new remote attack threats. As systems start to utilize more AI-based solutions, and as AI-supported cyberattacks are more likely to emerge in the near future, one possible cyber trend will involve increased attacks on critical infrastructure.

A failure in a system may cascade through other systems, which may be difficult to foresee.

Attacks designed to cause cascading effects are likely to inflict severe and widespread damage to societies. The disruption to, or destruction of, critical infrastructure would have an immediate impact on day-to-day life, societal safety and the economy. The eventual results can be far more severe than the effect on the initially affected system: loss of power can result in loss of communications, food, water, energy, and so forth. [3]

Actors who seek to cause severe damage to the critical functions of a society may be tempted to carry out attacks against critical infrastructure with cascading effects. Although critical infrastructures are commonly designed, implemented and maintained based on rigorous standards, it is not easy to identify all of the relevant factors contributing to cascading effects. New technologies introduce unknown vulnerabilities to hybrid threats when taken into use in real systems. A cascading effect might be the objective of hybrid threat activity aimed at destabilization, but also a means to an end. Attributing the attacker becomes more complicated when the cause and effect chain is extended. Moreover, cascading effects, when they create enough confusion, can function as a cover for hybrid threat operations in the same and/or other domains.

Another example of how AI can affect the cyber-physical domain concerns the way in which drones are harnessed to use facial recognition, for example, or other AI solutions to detect targets and deliver explosives to eliminate them for terrorist purposes. Drones may allow attackers to deploy or repurpose such systems for harmful ends, such as crashing fleets of autonomous vehicles, turning commercial drones into face-targeting missiles, or holding critical infrastructure to ransom. [4]

The rise of autonomous weapons systems on the battlefield risks the loss of meaningful human control and presents tempting targets for attack. The use of drones seems to be changing several perceptions connected to war. Drones can be argued to have lowered traditional disincentives for outside combat zone attacks. When an attack is launched from a distance without physical proximity, the perceived barrier of entry is lowered due to the disconnect. This can lead to an impression of the battlefield being 'global'.[5] Furthermore, the increased physical distance between the drone operator and the target appears to affect the moral judgement of the operator by increasing the dehumanization of the target.[6] This indicates that AI will increasingly enable war or interference mechanisms which bring the activity into the internal space of the target, while the 'battlefield' is viewed as global. Simultaneously, the human factor in operations will decrease, resulting in fewer human errors, but also potentially fewer decisions based on moral considerations.[7] This can even lead to the legal framework at both national and international levels being put under strain.

Irrespective of warfare, when coupled with AI as a tool of disruption, drones have significant power, and are an example of easily available tools that anyone can use to disturb the functioning of critical infrastructure. Airports are a case in point. For example, Gatwick Airport in London was completely shut down for 36 hours after drones were spotted flying in the immediate vicinity. The disruption had global cascading effects, and came with little or no cost to the perpetrators. [8]Drones are already efficient tools for actors engaging in hybrid threat activity, but combined with AI solutions, their destructive power could be multiplied.

3 Hybrid CoE Expert-pool discussion 2020.
4 Ibid.
5 The International Committee of the Red Cross, 'Drones and the challenges of remote warfare'.
6 Ibid.
7 Ibid.
8 Shackle, 'The mystery of the Gatwick drone'.

Increasing importance of AI in state-backed subversive psychological and information operations

AI's disruptive use potential in the political realm derives from the increased usage of cyberspace as a domain for, but also enabler of, politics. Detailed analytics, targeted propaganda, and cheap, highly believable fake videos present powerful tools for manipulating public opinion on previously unimaginable scales.

Micro-targeting in particular will be increasingly supported by AI. This means that the emergence of 'hyper-personalized influence targeting' (HPIT) will be used to achieve political, military and geopolitical objectives. HPIT has been used by Russian forces in Ukraine, for example, where a combination of electronic warfare equipment, commercial drone technology and fake mobile towers have been combined with psychological operations to intimidate citizens and sow mistrust.[9] It is highly probable that technology enabling HPIT will be accessible to state and non-state actors at a low cost in the future. This, combined with advancements in AI, will increase the accuracy and efficacy of microtargeting.

Developments in big-data harvesting will allow malicious actors to design and conduct HPITs on an industrial scale. State and non-state actors have the ability to harvest massive amounts of data by using AI. In a recent example, private Chinese company Zhenhua Data was shown to have harvested data on high-level individuals from Western countries. The Overseas Key Information Database (OKIDB) has been systematically collecting names since 2017 and currently contains over 2.4 million. The aim has been to gather details about countries' infrastructure, military deployments and public opinion, as well as an analysis of individuals with foreign military, political and business backgrounds.[10] Essentially, the use of AI to gather and comb through big data, combined with micro-targeting, blurs the traditional conceptual divide between the tactical and strategic levels.[11]

The ability to collect, analyze and act upon citizens' information at scale using AI could enable new levels of surveillance and invasions of privacy. This has the potential to fundamentally shift power between individuals, corporations and states. For example, an authoritarian state could use automated surveillance systems that utilize image and audio processing and combine this information with intelligence to control citizens and counter opposition.

Furthermore, the importance of visual information has increased in almost all information production, largely due to social media. The visualization of communication habits is not only visible in journalism and politics, but also in acts of violence such as the live streaming of terrorist attacks. Techniques for creating visual content are increasing and becoming easier to access, while traditional forms of video and image manipulation are rapidly improving. This points to a trend whereby the trustworthiness of visual and audio material will be increasingly contested. The decrease in trustworthiness can be observed, for example, in filters used to change the background of images, algorithms that credibly alter the features of the person in an image, and deepfake videos – created with deep-learning AI technologies – in which a person's face or body is digitally manipulated so that they appear to be someone else. Until now, the quality of the deepfakes has been mediocre and easy to spot, but high-end and highly realistic fakes will probably be accessible in the near future. The increasing visual information culture together with advances in AI will facilitate deception and disinformation operations. Audiences will be bombarded with individualized and manipulated messaging, meaning that tactical psychological operations are combined with strategic communications.[12]

China's social surveillance system can be cited as an example of a trend where data-driven technologies, facial recognition and AI enable the state to monitor and target people such as ethnic minorities and political opponents. These technologies can be used by corporations to allow people

9 Hybrid CoE, 'Trends in the Contemporary Information Environment'.
10 Sihi, 'Chinese firm harvests social media posts, data of prominent Americans and military'.
11 Hybrid CoE, 'Trends in the Contemporary Information Environment'.
12 Ibid.

to withdraw cash, check in at airports, and pay for goods purely through facial recognition. However, they are also used by the Chinese government to enforce its rule by monitoring and scoring its citizens. The authorities insist that the social scoring system allows them to improve security for citizens, using the commonly known "if you have nothing to hide you have nothing to fear" fallacy. In practice, however, using surveillance technologies to build a social scoring system is a tech-enabled way to wield political power through social and economic development, and to strengthen the power of the Communist Party.[13]

It is expected that AI-backed technology used for information operations will most often be employed by malicious actors under the threshold of war. This area of conflict legally and politically creates a grey zone that Western countries should respond to and aim to deter. In the absence of effective policies and organizational structures, the populations in Western democracies will increasingly fall victim to information operations by malicious actors.[14]

Issues to monitor

1. When will the first AI-supported cyberattack take place and due to what kind of events? How will attribution be carried out?
2. What are the interconnections between critical infrastructure in the cyber-physical systems? How can the possible cascading effects be anticipated, and what kind of actors have the capability, motivation and will to use cascading effects?
3. How will non-Western governments utilize AI? How will it be deployed against their own citizens? What kind of threat will this pose to Western countries? Will such technologies be exported to other countries with weak democracies, thereby contributing to further de-democratization?
4. How will Western states strike a balance between using technology to enable national security and protecting the privacy of their citizens?

13 Based on information from Liang et al., 'Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure'.
14 Hybrid CoE, 'Trends in the Contemporary Information Environment'.

TREND 2: Expansion of the role of cyber during times of crisis

Times of crisis have usually functioned as a magnet for cyber and information operations. This has been evident during the coronavirus pandemic, when the number of both cyber and information operations has increased. Hostile actors take advantage of crises, when society is focused on resolving the crisis rather than on combating external malicious activities. For example, the WHO reported that it has seen a fivefold increase in cyberattacks.[15]

The damage these operations can cause is not so much dependent upon the ingenuity of the attacker or propagandist, but on the resilience of the target. In fact, much of the malware used has been rather latent according to Interpol. The attacks reveal that old malware has been taking new forms, as well as using Covid-19 as a theme on which to build social engineering and disinformation tactics.[16]

The use of cyber during the pandemic

When it comes to the use of cyber, the actor aims to achieve its goals by targeting devices connected to cyberspace, by penetrating networks, spreading malware, or launching denial-of-service attacks. Through these actions, the actor is able to conduct espionage, prepare the battlefield for a possible conflict or war, steal or extort money, and disrupt vital functions of society in order to influence political decision-making. The actor may be a state, a criminal organization, a terrorist organization, or a group of activists.

Some attacks during the Covid-19 pandemic have been targeted at hospitals and medical research centres in an attempt to extort money through ransomware or information theft, or to gather intelligence about treatment, tests, and vaccines. Some attacks, on the other hand, target the end users, and take advantage of the fact that people try to find information about the coronavirus online and/or are working from home with insufficient protection in cyberspace.

For example, in the United Kingdom in early 2020, the criminals behind the Maze ransomware attacks targeted the Hammersmith Medicines Research facility (HMR). The HMR is a British company that has been on standby during the Covid-19 pandemic to perform the clinical trials for any coronavirus vaccine. The hacker group's mode of operation was to steal information from the target, inject malware that encrypts the target's systems, and then demand a ransom. If the target refused to pay, threats were made about publishing the stolen information online. In this case, as the HMR refused to meet the ransom demand, the hackers published thousands of former patients' records online on the dark web.

In March 2020, the Brno University Hospital in the Czech Republic was hit by a cyberattack, which disrupted operations at the hospital and forced it to reschedule surgeries. The hospital houses one of the largest coronavirus testing facilities in the Czech Republic. While recovering from the attack, the hospital lacked major ICT capabilities, such as data storage, which forced medics to make and transfer notes manually. While the various laboratories at the hospital were still able to function, there was no way to transfer the information to the database systems. As a result, processes slowed down, the lives of patients may have been endangered, and new patients had to be directed elsewhere.

Other EU member states as well as the US reported increased cyber activities during the pandemic. The US Health and Human Services

15 World Health Organization, 'WHO reports fivefold increase in cyber attacks, urges vigilance'.
16 Interpol, 'Global Landscape on COVID-19 Cyberthreat'.

Department suffered a cyberattack against its computer system, while the website of a public health department in Illinois with more than 200,000 registered clients was taken offline following a ransomware attack.

Both states and criminal groups have been connected to these attacks, which underlines the difficulty of attribution during a time of crisis. The challenge of attribution translates into the difficulty of obtaining and maintaining correct and up-to-date situational awareness, as well as coordinating responses. Some of the attacks during the crisis have apparently been backed by China, North Korea and Russia.[17] As an example, the UK National Cyber Security Centre has assessed that the Russian cyber threat actor APT29, also known as 'Cozy Bear' has attacked British organizations, such as drug companies and research groups working with vaccine development.[18] The hacker group has been identified by Britain, Canada and the US as "almost certainly" being part of Russian intelligence services.[19]

Discussion on whether cyber threat activity can be compared to strategic weapons and their potential for destruction in conventional warfare has been ongoing for a long time. Up to now, cyber threat activities have legally, as well as in the field of policy, been regarded as acts under the threshold of actual war. During the pandemic, the question of whether a cyberattack can be related to a conventional act of war has resurfaced again. Some of the attacks against critical health infrastructure, such as hospitals, have raised questions about the legal thresholds of cyber war.

Manipulative information interference during the pandemic

When talking about manipulative information interference, tools used by an actor to achieve its goals relate to targeting the cognition of the individual by using a device connected to cyberspace. This may be conducted by disseminating disinformation using services residing in cyberspace, such as social media. Through such actions, the actor is able, for example, to increase people's distrust in the government, healthcare system, the authorities, and fellow citizens. The actor may be a state, a criminal organization, a terrorist organization, or a group of activists.

As a consequence of openness and liberal values, Western societies are vulnerable to disinformation initiated by foreign state and non-state actors. The disinformation fed into the internal information system is also fuelled by domestic actors seeking political or economic gain.

As the coronavirus began to spread around the world, people started to search for information about it online. This opened up a new opportunity for malicious actors to exploit the situation in various ways. Websites have appeared that provide both accurate and inaccurate information. Some coronavirus scam examples include selling counterfeit medical equipment, not delivering purchased goods, fake charities, fake websites selling medical equipment, phishing attacks, and impersonations. There was, for example, a phishing attack in the name of the World Health Organization, and an impersonation case involving the Johns Hopkins University, which manages an interactive dashboard on coronavirus infections. Furthermore, in December 2020 the European Medicines Agency was subject to a cyberattack in which data including internal and confidential email correspondence was stolen, manipulated and leaked online. The leaked information included schematics of drug structures and correspondence about the evaluation processes of vaccines.[20] Correspondence that has been tampered with can constitute a useful disinformation tool, as the highly specific biotechnical language can easily sow mistrust among people who do not understand the specific jargon.[21]

The most provocative or interesting content starts circulating on the internet, feeding people's increased hunger for information, and creating what the World Health Organization has called an infodemic. The overabundance of information coming from a multitude of sources does not satisfy the

17 Wiggen, 'The impact of COVID-19 on cyber crime and state-sponsored cyber activities'.
18 National Cyber Security Centre, 'UK and allies expose Russian attacks on coronavirus vaccine development'.
19 Ibid.
20 European Medicines Agency, 'Cyberattack on EMA – update 5'.
21 Lomas, 'EMA warns over doctored COVID-19 vaccine data hacked and leaked online'.

need to gain information, but rather makes it more difficult for people to know what to trust.[22]

During the pandemic many different ways of disseminating disinformation have been observed; on social media four main account types have been identified: authentic human accounts, accounts operated by bots, cyborg accounts run partly by bots and partly by human users, and stolen and hacked accounts.

Disinformation may also be used during a crisis to incite physical attacks against infrastructure with the aim that action incited online will turn into offline action. During the coronavirus pandemic, there has been an increase in arson attacks against 5G masts, for example. Ever since 5G technology became viable in 2019, the fear that 5G radiation causes health problems has proliferated on social media. Disinformation video clips that feature people appearing as experts explaining the health hazards, or dead birds next to 5G towers, started to emerge. In 2020, matters took a more drastic turn as anti-5G groups started spreading rumours that 5G had caused the coronavirus outbreak, and that the virus could be transmitted over 5G waves or was likely to spread more quickly in areas with 5G connections. This resulted in physical harassment of telecom engineers, and in arson attacks against base stations in several European countries.

However, any criminal activity is relevant when it comes to responding to hybrid threats, for several reasons. First of all, when they occur on such a massive scale as they have done during the pandemic, they obscure the situational awareness and hinder the attribution of hybrid threat actors. The more actors and motives included in the picture, the more difficult it becomes to differentiate between relevant hybrid threat activity and strategic behaviour with escalation potential and, for example, criminals motivated by monetary gain or fame in the short term.

Secondly, cyberattacks against institutions, and scams perpetrated in the guise of distinguished organizations leading the discussion, such as the WHO, influence people's sentiments and create vulnerabilities that hybrid threat actors can exploit. One way to counter hybrid threats is to increase the overall societal resilience, which entails trust in organizations and institutions, which must duly earn this trust. Should they fail to respond to and mitigate the effects of such scams, this would damage their credibility and people's trust in them, and compromise societal resilience.

Issues to monitor

1. Lessons learnt from the coronavirus pandemic about malicious behaviour in cyberspace.
2. Interfaces between the domains of cyber, society and security; will the widespread and effective use of cyber and manipulative information interference affect how people perceive the role and trustworthiness of institutions in future crises?
3. How states change the way they attribute and respond to malign cyber and information activities, especially when they occur during a time of crisis.
4. The gaps in international collaboration in the cyber domain, which is required to protect critical functions while dealing with a crisis.
5. Interfaces between the information and cyber domains and the physical realm; can violent hostility against 5G be utilized, or even replicated by a hostile actor against other technological advancements in Western countries?

22 World Health Organization, 'Managing the COVID-19 infodemic: Promoting health behaviours and mitigating the harm from misinformation and disinformation'.

TREND 3: Growth in dependencies between policy and technology

There has typically been little dialogue between policymakers and technology developers, who have increasingly influenced developments in the cyber domain. Technology has always developed more rapidly than policy and legislation, and the pace is increasing exponentially.

According to leading cyber security expert Bruce Schneier, "policy is how society mediates how individuals interact with society, whereas technology has the potential to change how individuals interact with society." [23] Constant friction exists between technology and policy, a situation caused by technologists perceiving policymakers as constantly being in the way of innovation, and policymakers continuously demanding that technologists should slow their pace and conform to policies more obediently.[24] However, as the emerging technologies become more vital to society and technology companies take actions that policymakers may not have considered, it is clear that dependencies between technology companies and the policy side are growing, which creates new challenges for both. A constructive dialogue is needed between policymakers and technology developers for the purposes of economic growth, social development, and state security.

With the proliferation of 5G technology, the discussion around the use of technology from "third states" has emerged on a larger scale than ever before and is perhaps one of the best examples of how policy and technology have become interdependent. The discussion has revolved around China and Huawei up to now, but the issue could and should be generalized as emerging technologies are deployed, especially for critical functions. One of the questions technologists and policymakers should address is whether technology acquired from a manufacturer from another state can be trusted not to pose a risk to national security by providing not only a back door, but rather a front door to the critical infrastructure of the state. This possible "cultural coding" of technology will increase the dependencies between policymakers and technology companies.

As a result of the China and Huawei case, several Western states had to have a technology and policy dialogue addressing the issue. On the one hand, deploying 5G is seen as important from an economic and functional perspective. On the other hand, deploying technology that may not be trustworthy could pose a risk to national security. While some Western states have banned the use of Huawei technology completely, some make compromises by allowing non-sensitive parts of the infrastructure to contain a limited amount of Huawei equipment. However, some states already have Huawei equipment installed, and changing it would be expensive. Moreover, the European Union has had to address the issue of 5G technology by conducting a risk assessment, leading to an EU toolbox [25]outlining how to securely deploy 5G in the EU.

Another example of dependency between policy and technology are manipulative information interference activities. In 2018, as a response to the European Commission's objectives to tackle disinformation, representatives of online platforms, leading social networks, advertisers and the advertising industry agreed on a self-regulatory Code of Practice to address the spread of online disinformation and fake news.[26] This code is, as the name suggests, self-regulatory, underlining the responsibility of the social media companies. Furthermore, on 15 December 2020, the EU published the Digital Services Act Package, which pro

23 Schneier, 'Policy vs. Technology'.
24 Ibid.
25 European Union, 'Transport cybersecurity toolkit'.
26 European Commission, 'Code of Practice on Disinformation'.

poses two pieces of legislation that aim to protect citizens on online platforms: the Digital Services Act aims to create a framework to handle illegal or potentially harmful content on online platforms by increasing transparency, while the Digital Markets Act aims to regulate large online platforms in their role as gatekeepers of online markets.[27] Both of these regulatory projects illustrate the need to maintain a dialogue between policymakers and technology companies.

The 5G and disinformation issues have highlighted the new dependencies between policymakers and technology developers, at both national and international levels, which may serve to point the way to much-needed discussion on other topics as well. Another emerging technology family that merits similar discussion is artificial intelligence. A report on the dual use of artificial intelligence calls for policymakers and technology experts to work together to understand and prepare for the malicious use of AI, and to actively expand the range of stakeholders engaging in preventing and mitigating the risks of its malicious use.[28] Further, the EU's recent white paper on artificial intelligence[29] serves as an example of balancing between policy and technological development. These are strong indicators that the cyber domain has produced a new type of dependency in democratic states with liberal economies. This has likewise resulted in calls for dialogue between policymakers and technology developers. As examples of national and international efforts start to bear fruit, states and international organizations should strive to establish more structured forms of dialogue to enable a balance between policy and technology in an environment where technological change is led by private companies.

Issues to monitor

1. What are the main drivers of dialogue between policymakers and technology companies?
2. How will the European Commission's Code of Practice on Disinformation be followed and how will the newer platforms be included in it?
3. What might cause discussion, similar to that which revolved around 5G, to emerge in other areas as well, such as AI?
4. What structural forms could emerge to enable discussion on the balance between policy and technology?

27 European Commission, 'The Digital Services Act package'.
28 Brundage et al., 'The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation'.
29 European Commission, 'On Artificial Intelligence'.

Conclusions

The three trends identified in this report – **increase in the disruptive use of artificial intelligence**; **expansion of the role of cyber during times of crisis**; and **growth in dependencies between policy and technology** – all highlight the changes that the cyber domain has brought about in the security environment.

The trend reflecting an *increase in the disruptive use of artificial intelligence* shows how AI has created new tools for disruptive use. The cyber-physical domain has given rise to new features where AI-supported cyberattacks are likely to emerge in the form of increased attacks against critical infrastructure with the aim of creating cascading effects. A similar idea depicting the transfer of action from online to offline can be identified in the use of disinformation during the Covid-19 crisis to incite attacks against infrastructure, covered under the *expansion of the role of cyber during times of crisis* trend. This means that more unexpected events and cascading effects are likely in the near future when AI is used in disruptive ways. Furthermore, drones, big data possibilities, micro-targeting, and deep fakes are also changing the understanding of war, privacy and influencing. While AI can provide many benefits in the future, it also has a dark side and its disruptive use could prove to be a real challenge to counter.

The trend indicating an *expansion of the role of cyber during times of crisis* has become highly visible during the Covid-19 pandemic when different cyber and manipulative information interference activities increased. This highlights how the tools that cyber enables are becoming an integral part of the toolkit used by hostile actors, and how the security environment during a crisis becomes even more challenging, indicating that hostile actors are increasingly viewing crisis situations as an opportunity to enhance their own strategic interests. Added to this, hostile actors themselves are able to draw lessons from the crisis, and the malicious activity in cyberspace will continue to evolve and affect phenomena outside the cyber domain, such as health hazards.

The trend pointing to a *growth in dependencies between policy and technology* also demonstrates the way in which cyber has affected the relationship between the public and the private sector. It is a new situation for both sides but the increasing dependencies are clear. Without a constant dialogue between the policy side and different technology companies (including social media), the dependencies might erode the basic principles of democratic systems and liberal economies. This is, after all, the primary aim of hostile actors behind the malign use of the cyber domain.

APPENDIX 1: List of contributors

Catharina Candolin (main author), Special Advisor, Defence Command Finland

Stephanie Carvin, Assistant Professor, Norman Paterson School of International Affairs, Carleton University

Eugenio Cusumano, Lecturer in International Relations, Leiden University

Guillaume Lasconjarias, Research Fellow, Institut Français des Relations Internationales

Lauri Lindström, Researcher, NATO CCD COE

Madeleine Myatt, Research Associate, University of Bielefeld, RTG "World Politics"

Reijo Savola, Principal Scientist, VTT Technical Research Centre of Finland

Mariëlle Wijermars, Assistant Professor in Cyber-Security and Politics, Maastricht University

Hanna Smith, Director of Strategic Planning and Responses, Hybrid CoE

Josef Schroefl, Deputy Director, Community of Interest of Strategy and Defence, Hybrid CoE

Emma Lappalainen, Coordinator, Hybrid CoE

Jarno Välimäki, Coordinator, Hybrid CoE

Bibliography

Bennhold , Katrin & Ewing, Jack. 'In Huawei Battle, China Threatens Germany 'Where It Hurts': Automakers'. *The New York Times*, 16 January, 2020. https://www.nytimes.com/2020/01/16/world/europe/huawei-germany-china-5g-automakers.html. Last accessed 24 March, 2021.

Brundage, Miles 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, University of Cambridge, Center for a New American Security, Electronic Frontier Foundation, OpenAI, February 2018. https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217. Last accessed 24 March, 2021.

Center for Strategic and International Studies. 'Significant Cyber Incidents since 2006'. https://csis-website-prod.s3.amazonaws.com/s3fs-public/210226_Significant_Cyber_Events.pdf?_zgMwQn.ZIQIHWCMGNMZfZJhjcypWe6s. Last accessed 24 March, 2021.

Commission Recommendation (EU) 2019/534 of 26 March 2019 on the cybersecurity of 5G networks; OJ L 88, 29.3.2019, p. 42-47. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019H0534. Last accessed 24 March, 2021.

Czuczka, Tony & Arons, Steven. 'China Threatens Retaliation Should Germany Ban Huawei 5G'. Bloomberg, 15 December, 2019. https://www.bloomberg.com/news/articles/2019-12-14/china-threatens-germany-with-retaliation-if-huawei-5g-is-banned. Last accessed 24 March, 2021.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148. Last accessed 24 March, 2021.

European Commission. 'Code of Practice on Disinformation', 26 September, 2018. https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation. Last accessed 24 March, 2021.

European Commission. 'Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, Secure 5G deployment in the EU - Implementing the EU toolbox'. Brussels, 29 January, 2020. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64481. Last accessed 24 March, 2021.

European Commission. 'Cybersecurity package 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'', 19 September, 2017. https://ec.europa.eu/digital-single-market/en/news/cybersecurity-package-resilience-deterrence-and-defence-building-strong-cybersecurity-eu. Last accessed 24 March, 2021.

European Commission. 'On Artificial Intelligence – a European approach to excellence and trust'. White Paper, 19 February, 2020. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf. Last accessed 24 March, 2021.

European Commission. 'The Digital Services Act package', 19 January, 2021. https://ec.europa.eu/digital-single-market/en/digital-services-act-package. Last accessed 24 March, 2021.

European Medicines Agency. 'Cyberattack on EMA – update 5'. News, 15 January, 2021. https://www.ema.europa.eu/en/news/cyberattack-ema-update-5. Last accessed 24 March, 2021.

European Union. 'Transport cybersecurity toolkit', 2020. https://ec.europa.eu/transport/sites/transport/files/cybersecurity-toolkit_en.pdf. Last accessed 24 March, 2021.

Giannopoulos, Georgios et al. 'The Landscape of Hybrid Threats: A conceptual model, public version'. EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021. doi:10.2760/44985, JRC123305. Last accessed 24 March, 2021.

Gilding, Simeon. '5G choices: a pivotal moment in world affairs'. Australian Strategic Policy Institute, The Strategist, 29 January, 2020. https://www.aspistrategist.org.au/5g-choices-a-pivotal-moment-in-world-affairs/. Last accessed 24 March, 2021.

Hoffman, Samantha & Kania, Elsa. 'Huawei and the ambiguity of China's intelligence and counter-espionage laws'. Australian Strategic Policy Institute, The Strategist, 13 September, 2018. https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/. Last accessed 24 March, 2021.

Hybrid CoE. 'Trends in the Contemporary Information Environment'. Hybrid CoE Trend Report, 4 May, 2020. https://www.hybridcoe.fi/wp-content/uploads/2020/05/Hybrid-CoE-Trend-Report-4.pdf. Last accessed 24 March, 2021.

The International Committee of the Red Cross. 'Drones and the challenges of remote warfare'. International Review of the Red Cross. https://e-brief.icrc.org/issue/new-technologies-and-the-modern-battlefield-humanitarian-perspectives/part-2-drones/. Last accessed 24 March, 2021.

Interpol. 'Global Landscape on COVID-19 Cyberthreat', April 2020. https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats. Last accessed 24 March, 2021.

Kim, Christine. 'North Korea hacking increasingly focused on making money more than espionage: South Korea study'. Reuters, 28 July, 2017. https://www.reuters.com/article/us-northkorea-cybercrime/north-korea-hacking-increasingly-focused-on-making-money-more-than-espionage-south-korea-study-idUSKBN1AD0BO. Last accessed 24 March, 2021.

Liang, Fan et al. 'Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure'. *Policy and Internet* 10(4), 415-453. https://doi.org/10.1002/poi3.183. Last accessed 24 March, 2021.

Lomas, Natasha. 'EMA warns over doctored COVID-19 vaccine data hacked and leaked online'. *Techcrunch*, 15 January, 2021. https://techcrunch.com/2021/01/15/ema-warns-over-doctored-covid-19-vaccine-data-hacked-and-leaked-online/. Last accessed 24 March, 2021.

Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge: Cambridge University Press, 2018.

National Cyber Security Centre. 'UK and allies expose Russian attacks on coronavirus vaccine development'. News, 16 July, 2020. https://www.ncsc.gov.uk/news/uk-and-allies-expose-russian-attacks-on-coronavirus-vaccine-development. Last accessed 24 March, 2021.

Office of the Director of National Intelligence. 'A guide to cyber attribution'. 14 September, 2018. https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf. Last accessed 24 March, 2021.

O'Flaherty, Kate. 'The Iran Cyber Warfare Threat: Everything You Need To Know'. Forbes, 6 January, 2020. https://www.forbes.com/sites/kateoflahertyuk/2020/01/06/the-iran-cyber-warfare-threat-everything-you-need-to-know/. Last accessed 24 March, 2021.

Panetta, Kasey. 'Gartner's Top 10 Security Predictions 2016'. Gartner, 15 June, 2016. https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/. Last accessed 24 March, 2021.

Roberts, Stuart. 'Global AI experts sound the alarm. Leading researchers co-author unique report warning of the malicious use of AI in the coming decade'. University of Cambridge. https://www.cam.ac.uk/Malicious-AI-Report. Last accessed 24 March, 2021.

Schneier, Bruce. 'Policy vs. Technology'. Schneier on Security, 21 February, 2020. https://www.schneier.com/blog/archives/2020/02/policy_vs_techn.html. Last accessed 24 March, 2021.

Shackle, Shamila. 'The mystery of the Gatwick drone'. *The Guardian*, 1 December, 2020. https://www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone. Last accessed 24 March, 2021.

Sihi, Gerry. 'Chinese firm harvests social media posts, data of prominent Americans and military'. *The Washington Post*, 14 September, 2020. https://www.washingtonpost.com/world/asia_pacific/chinese-firm-harvests-social-media-posts-data-of-prominent-americans-and-military/2020/09/14/b1f697ce-f311-11ea-8025-5d3489768ac8_story.html. Last accessed 24 March, 2021.

United Nations Office for Disaster Risk Reduction. 'Resilience'. Terminology. https://www.undrr.org/terminology/resilience. Last accessed 24 March, 2021.

Wiggen, Johannes. 'The impact of COVID-19 on cyber crime and state-sponsored cyber activities'. Konrad Adenauer Stiftung Facts & Findings No 391, June 2020. https://www.kas.de/documents/252038/7995358/The+impact+of+COVID-19+on+cyber+crime+and+state-sponsored+cyber+activities.pdf/b4354456-994b-5a39-4846-af6a0bb3c378?version=1.0&t=1591354291674. Last accessed 24 March, 2021.

World Health Organization. 'Managing the COVID-19 infodemic: Promoting health behaviours and mitigating the harm from misinformation and disinformation'. Statement, 23 September, 2020. https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation. Last accessed 24 March, 2021.

World Health Organization. 'WHO reports fivefold increase in cyber attacks, urges vigilance'. News release, 23 April, 2020. https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance. Last accessed 24 March, 2021.


Hybrid CoE