

CONNECTIONS

THE QUARTERLY JOURNAL

CONNECTIONS SPECIAL EDITION



PARTNERSHIP FOR
PEACE CONSORTIUM
OF DEFENSE
ACADEMIES AND
SECURITY STUDIES
INSTITUTES

NATIONAL CYBER DEFENSE POLICIES

CHALLENGES AND THE WAY FORWARD

WINTER 2020

*Partnership for Peace Consortium of
Defense Academies and Security Studies
Institutes*

The PfP Consortium Editorial Board

Sean S. Costigan	Editor-In-Chief
Marcel Szalai	Managing Editor
Aida Alymbaeva	International University of Central Asia, Bishkek
Pal Dunay	George C. Marshall Center, Garmisch-Partenkirchen
Philipp Flury	Geneva Centre for Security Policy, Geneva
Piotr Gawliczek	Cuiavian University in Wloclawek, Poland
Hans-Joachim Giessmann	Berghof Foundation, Berlin
Dinos Kerigan-Kyrou	Joint Command & Staff Course, Military College, Irish Defence Forces
Chris Pallaris	i-intelligence GmbH, Zurich
Tamara Pataraiia	Civil Council of Defense and Security, Georgia
Todor Tagarev	Bulgarian Academy of Sciences, Sofia
Eneken Tikk	Cyber Policy Institute, Jyväskylä

The views expressed and articles appearing in all *Connections* publications are solely those of the contributing authors and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

This edition is supported by the United States government. It was compiled with the assistance and support of Gili Perl, International Cooperation Policy Officer, Cyber Defence Command, Austria.

The Consortium's family of publications is available at no cost at <http://www.connections-qj.org>. If you would like to order printed copies for your library, or if you have questions regarding the Consortium's publications, please contact the PfPC at PfPCStratCom@marshallcenter.org.

Dr. Raphael Perl
Executive Director

Sean S. Costigan
Editor-In-Chief and Chair, Editorial Board



ISSN 1812-1098, e-ISSN 1812-2973

CONNECTIONS

THE QUARTERLY JOURNAL

Vol. 19, no. 1, Winter 2020



Contents

Vol. 19, no. 1, Winter 2020

Policy Highlights

- National Cyber Defence Policies and the Role of International Cooperation 5
Colonel Jaak Tarien

National Policies

- Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr 9
Lieutenant General Ludwig Leinhos
- Austria's National Cyber Security and Defense Policy: Challenges and the Way Forward 21
Major General Hermann Kaponig
- Responding to the Cyber Threat: A UK Military Perspective 39
Air Commodore Phil Lester and Captain Sean Moore
- Israel Defense Forces and National Cyber Defense 45
Lior Tabansky
- Cybersecurity in Switzerland: Challenges and the Way Forward for the Swiss Armed Forces 63
Marie Baezner

Practitioners' and Academic Perspectives

- National Cyber Security Strategy and the Emergence of Strong Digital Borders 73
Sanjay Goel

How Improved Attribution in Cyber Warfare Can Help De-escalate Cyber Arms Race <i>Sanjay Goel</i>	87
--	----



Policy Highlights

National Cyber Defence Policies and the Role of International Cooperation

Colonel Jaak Tarien

Director of the NATO Cooperative Cyber Defence Centre of Excellence

Digitalization has made our societies vulnerable to cyber threats – from electric grids to elections. This is also true for militaries, and cyber defence has become a natural task for all defence organizations. Cyber threats cannot be considered as new threats anymore. However, the cyber threat landscape is changing rapidly, and will continue to do so. Malicious viruses, hackers, hacking, etc., are still part of this landscape, but cyber weapons and cyberattacks originating from nation states are the primary security concerns today. Malicious actors are quick to learn from each other and their tools proliferate. How should we respond? The creation of more secure cyberspace is possible only through cooperation. As there are no traditional borders in cyberspace, NATO Allies and Partners share the same responsibilities, as well as opportunities.

Cooperation in the area of cyber defence was, as it clearly appears from the name, the primary motivator behind the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) by six NATO nations in 2008. As of today, the Centre is staffed and financed by 25 countries altogether. Belgium, Bulgaria, the Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Spain, Turkey, the United Kingdom and the United States are signed up as Sponsoring Nations of the NATO CCD COE. Austria, Finland and Sweden are Contributing Participants, a status eligible for non-NATO nations. The Centre continues to attract new members: Japan, Croatia, Montenegro, Slovenia and Switzerland are in the process of joining the Centre. In addition, Canada, Luxembourg and Australia have announced their intention of accession.

The NATO CCD COE, focusing on research, training and exercises, offers various training courses at a technical, operational, and strategic level for its member nations. In addition, the International Law of Cyber Operations Course is prepared for legal advisors. The Centre conducts a yearly international Red Team vs Blue Team exercise *Locked Shields* for cybersecurity experts to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks. *Locked Shields* also includes a strategic element that covers decision-making, legal, and communication aspects. More than 1500 experts from 30 nations took part in *Locked Shields* 2019. *Crossed Swords*, another annual exercise, is a technical red-teaming cyber exercise targeting penetration testers, digital forensics experts and situational awareness experts. The annual conference CyCon—International Conference on Cyber Conflict—is the Centre’s contribution to the broader cybersecurity community. CyCon promotes research and development on the technical, legal, policy, strategy, and military perspectives of cyber defence and security. One of the internationally recognized research accomplishments for the Centre has been the “Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.”¹ The Tallinn Manual 2.0 is the most comprehensive analysis of how existing international law applies to cyberspace. Finally, since 2018 the Centre is responsible for identifying and coordinating education and training solutions in cyber defence for all NATO bodies across the Alliance. As the Centre’s heart is its international staff, cyber experts with various backgrounds, then all our deliverables are practical examples of the value and benefits of international cooperation.

The importance of cyberspace for our societies and economies will only grow. It is still transforming – connecting increasingly more people and devices, new emerging technologies allow new functionalities. But the future of cyberspace is in our hands. This growth and development are only possible if security and safety of, and in, cyberspace are provided. This means that our national policies, strategies, and laws need continuous review and adaptation. Cybersecurity will remain a challenge for all governments and globally. We will see discussions on roles and responsibilities of different state institutions, including military, on how to best respond to this challenge.

In this issue of “Connections,” perspectives from Austria, Germany, Israel, Switzerland, the UK and the US are all valuable reference materials for other nations.

The more ambitious goal—more secure and safe cyberspace as a whole—is only possible through international cooperation. NATO and the EU, and other organizations, have a significant role here. Yes, international cooperation in cybersecurity is a sensitive and complex issue, and there are limits. However, the very basis for this cooperation is trust, information sharing and the ability to learn from each other. If we succeed with this, then the door for further coop-

¹ Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Second edition (Cambridge, UK: Cambridge University Press 2017).

eration is open. The current issue of “Connections” is another step toward opening this door further.

Disclaimer

The views expressed are solely those of the contributing author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium’s editors.

About the Author

Colonel **Jaak Tarien** is the Director of the NATO Cooperative Cyber Defence Centre of Excellence, based in Estonia, since September 2018. Prior to joining the Centre Colonel Tarien served as the Commander of the Estonian Air Force from August 2012 to July 2018. Among other assignments, he has also served as Staff Officer with NATO’s Supreme Allied Command Transformation (ACT), as Deputy Director of the Regional Airspace Surveillance Coordination Centre and as the Commander of the Estonian team at the BALTNET Regional Airspace Surveillance Co-ordination Centre in Lithuania.

Colonel Tarien, a graduate of the United States Air Force Academy, earned his Master’s degree from the Air Command and Staff College of the USAF Air University. He recently also acquired a Master of Science degree in National Resource Strategy at the US National Defence University.



Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr

Lieutenant General Ludwig Leinhos

Cyber and Information Domain Service, Bundeswehr, Germany

Abstract: Current conflicts are increasingly carried out in hybrid forms, including attacks on technical networks and campaigns aimed at influencing public opinion. The Bundeswehr has responded to this development by pooling its capabilities in this field and combining them in the new Cyber and Information Domain Service. On par with the classic service branches—Army, Air Force, and Navy—this service, with its approximately 14,500 members, makes an important contribution to the whole-of-government security provision.

Keywords: cyber domain, cyber operations, critical infrastructure, hybrid threat, joint fusion centre.

Policy Highlights

In Germany, the provision of cybersecurity—i.e. a condition where risks from cyberspace have been reduced to an acceptable minimum—is a whole-of-government task. This is laid down in the 2016 White Paper,¹ the current basic document on German security policy. There are few areas where internal and external security are as closely intertwined as they are in cyberspace. This includes the joint protection of critical infrastructure.

Nevertheless, even within a whole-of-government approach, there exist areas of responsibility. The Federal Ministry of the Interior, for instance, is responsible for cybersecurity and the protection of civilian infrastructure. It also has the lead responsibility for Germany's cybersecurity strategy. The Federal Foreign Of-

¹ "White Paper on German Security and the Bundeswehr," 2016, <https://issat.dcaf.ch/download/111704/2027268/2016%20White%20Paper.pdf>.

fice shapes international cybersecurity policy, while the Federal Ministry of Defence is responsible for cyber defence.

In order to conduct its operations, the Bundeswehr, as a military organization, particularly depends on the availability, confidentiality, and integrity of data, IT-based services, and network-enabled infrastructure. For this reason, Bundeswehr cyber defence places particular emphasis on the protection of friendly systems. An essential instrument to ensure this is a comprehensive, digitally generated, situation picture that also includes information space and is made available to other government agencies as part of a network-enabled approach. In information space, people perceive, interpret, and spread information beyond the technical sphere. What is known as “published opinion” is an essential aspect of our considerations.

Apart from preventive measures, reactive and active measures (cyber and information domain operations) may also become necessary when it comes to ensuring the protection of friendly systems. Cyber and information domain operations can take the form of independent as well as supporting operations. In a conflict, they present a conceivable option for initial operations, which can, if necessary, even be conducted at a time when conventional forces have not yet been alerted. Cyber and information domain operations are subject to the same legal constraints as those of other Bundeswehr forces.

In addition to the whole-of-government approach, multinationality is another basic principle of German cyber defence – as well as German security policy in general. Here, we aim at working together with EU and NATO partners as well as in a bilateral, multilateral, and UN framework to ensure cybersecurity and establish the accompanying legal framework.

Policy Challenges

The German Federal Government regards threats from cyber and information space as one of the key challenges facing German security policy. Digitalization has penetrated all areas of life and together with the increasing interconnectedness of individuals, organizations, and states, this offers unique opportunities. At the same time, however, it leaves governments, societies, and economies particularly vulnerable.

Since its 2016 Warsaw Summit,² NATO has viewed cyberspace as an independent domain of operations – similar to the land, air, sea, and space domains. In cyberspace, armed forces can use suitable software to reconnoitre and subsequently engage enemy systems, amongst other things. In practical terms, this could entail, for example, the interruption of logistic chains, the corruption of data crucial to operations, or the restriction of the availability of key enemy C2 and information systems.

² “NATO Warsaw Summit Communiqué,” July 2016, paras 70-71, www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber.

By including not only the electromagnetic spectrum but also and especially information space, the Bundeswehr has deliberately defined this new military domain in a more comprehensive way than NATO does. Activities in the information environment, such as fake-news campaigns, continue to increase, making it possible to deliberately stir up unrest. International and national conflicts are more and more influenced by propaganda and disinformation. Consequently, information is becoming one of the core resources of the future.

The cyber and information domain distinguishes itself from the classic domains of operations by several unique features. It is characterized by a high degree of complexity. Territoriality is complemented by virtual reality. The cyber and information domain cannot be divided into combat sectors with clear spatial boundaries. The same holds true for the manoeuvring of troops. Nevertheless, physical effects can be achieved in the cyber and information domain, too. The place where cyber and information domain operations create an effect, however, can be tens of thousands of kilometres away from where the action was initiated. Time, too, plays a different role, considering that effects in cyberspace can be achieved over any distance without delay. Given sufficient preparation, effects are produced in near real-time.

The attribution of attacks poses a problem. Thanks to the available technical possibilities, actions can be concealed extremely well. In addition, there are a large number of possible perpetrator groups and motives. By now, the possibilities of digitalization have made it possible for non-state actors to achieve effects by way of cyberattacks which previously could only be achieved by state actors.

To sum up, today's conflicts are essentially characterized by their hybrid nature. Attacks in cyberspace and disinformation campaigns that remain below the threshold of armed attacks need to be taken into consideration just as much as the massive use of cyber operations as part of a national and collective defence scenario. A clear analysis leading to an informative situation picture is, therefore, of essential importance.

As Chief of the Cyber and Information Domain Service, I see it as my responsibility not to confine myself to minimizing the risks described above. For the Bundeswehr, digitalization also offers enormous opportunities, which will be discussed below.

Policy Implementing Structures and Whole-of-Nation Context

Possible threats to governments, economies and societies are multi-faceted and include data theft, espionage, damage of critical infrastructure, disruption of government communications and are as diverse as the agencies that deal with them. Often hybrid strategies are used to exploit the interfaces between responsibilities, for instance, between internal and external security.

Therefore, the closing of ranks and a system of exchange at national level are an absolute necessity. At the strategic level of the state's cybersecurity architecture, the responsibility for coordinating the cooperation within the Federal Government as well as between the government and the business sector rests with

the National Cyber Security Council. At the operational level, the National Cyber Response Centre, a forum to promote the cooperation of government agencies in the cyber and information domain, was established as early as 2011 under the auspices of the Federal Office for Information Security, which is subordinate to the Federal Ministry of the Interior. In cooperation with all key actors, the National Cyber Response Centre is currently undergoing further adaptation towards an interagency operational-level institution. This is an essential step towards establishing even more efficient structures for ensuring Germany's future ability to act in this field. Here, the involvement of national Internet service providers, too, is indispensable. As a representative of the Bundeswehr, the Cyber and Information Domain Service actively contributes to this process. Once the further adaptation of the National Cyber Response Centre has been completed, it could be used to disseminate information provided by the new Joint Cyber and Information Domain Fusion Centre.

In order to make a vital contribution to cybersecurity in Germany as early as during the development stage of key technologies, the Federal Ministry of Defence and the Federal Ministry of the Interior have been working together to build up the Agency for Innovation in Cyber Security since late 2018. This agency will award targeted contracts for ambitious research projects with high innovation potential. In this way, it will be able to tread new paths in order to maintain Germany's prominent role in technological innovation.

With the Cyber Innovation Hub, the Federal Ministry of Defence has its own interface between the start-up scene and the Bundeswehr.

The Federal Office for Information Security provides support to government institutions, such as the German Bundestag, on issues of information security. If required, it dispatches computer emergency response teams to re-establish information security as quickly as possible. For the Bundeswehr, this task is performed by the Cyber and Information Domain Service.

The attribution—i.e. the identification of the perpetrators—of a cyber-attack primarily falls within the responsibility of law enforcement agencies in cooperation with the intelligence services.

As long as the Bundeswehr is not itself affected by a cyberattack, the German Basic Law limits its role to the provision of administrative assistance and support in the event of particularly grave accidents. This does not mean, however, that a serious attack on critical infrastructure cannot result in a military response in the context of national and collective defence.

Policy Implementation

Protection & Operations, Reconnaissance & Effects, Geospatial Information

The Bundeswehr has been closely concerned with the issue of information security since the 1990s. For more than 20 years, it has run its own IT security organization, which it is currently developing into a comprehensive information secu-

rity organization, placing a particular emphasis on raising awareness about the utilization of IT equipment among Bundeswehr members. In response to the effects of increasing digitalization, the new German Cyber and Information Domain Service was inaugurated in April 2017. This major organizational element currently comprises approximately 14,500 military and civilian personnel. It has pooled established units with relevant expertise and expanded existing know-how.

The task spectrum of this major organizational element is very diverse. One focus of its activities is the protection and operation of the Bundeswehr IT system both at home and in theatre. Its capabilities are not limited to establishing the required connections; it also has situation centres that monitor the IT system around the clock. This is where attacks are detected and, if necessary, contained. In addition, before IT systems and systems with IT components can be employed in the Bundeswehr, they are tested and accredited by a central agency with regard to information security.

The overall responsibility for information security in the Bundeswehr rests with the Bundeswehr Chief Information Security Officer (CISOBw) who also acts as my deputy in the position of Vice Chief of the Cyber and Information Domain Service.

Capabilities for reconnaissance and effects in cyber and information space are also being strengthened and further developed. This includes cyber operations, such as the infiltration of enemy IT networks and the detection of vulnerabilities in friendly systems. Military intelligence provides evaluated reconnaissance results, for instance, radar imagery tailored to specific requirements or high-resolution images for the protection of own and allied forces. Electronic warfare and operational communications are also included in the capabilities of the Cyber and Information Domain Service. Operational communication looks at the factors of information and perception, such as: What do people in theatre say about military operations? Is false information circulating about the Bundeswehr? Once these questions are answered, countermeasures can be taken, if necessary.

The members of the Geoinformation Service assist all areas of the Bundeswehr in achieving their mission by providing high-resolution, quality-assured, digital and analogue geospatial information of all kinds.

Joint Cyber and Information Domain Fusion Centre

The complexity of cyber and information space makes sound analysis indispensable. For this reason, the Cyber and Information Domain Service has established its own situation centre for the cyber and information domain. Through the fusion of existing (partial) situation pictures from all functional areas relevant to the cyber and information domain, the Joint Cyber and Information Domain Fusion Centre generates a valid situation picture that forms the basis for determining possible courses of action and exploiting synergy effects. Analysts process various types of data—both structured and unstructured—from different sources; in future, they will also make use of artificial intelligence and big data

methods. For instance, by correlating data from the Bundeswehr IT system with other military intelligence information as well as open-source information gathered from social networks, conclusions can be drawn that can indicate a growing hybrid threat or a coordinated cyber-attack. The analyses thus obtained can then be made available to users in the Bundeswehr and also to other government agencies.

Software Expertise in the Bundeswehr

The Bundeswehr Cyber and Information Domain Service is capable of developing its own software as well as adapting commercially available software products to Bundeswehr or NATO requirements. Since 1 April 2019, the Bundeswehr Centre for Software Expertise has pooled these capabilities and continues to develop them. The inherent possibilities can hardly be overestimated. This allows us to make a decisive contribution to digitalization in the Bundeswehr – from the equipment of commando forces and combat posts to Bundeswehr data centres. One outstanding example—just one of many—is the harmonization of C2 information systems. The Bundeswehr has harmonized the existing C2 information systems of the armed forces, adapting them for service orientation. This project, as well as the succeeding projects that build on it, such as the German Mission Network, will enable the Bundeswehr to provide the majority of its mission-oriented IT from data centres through a “Bundeswehr private cloud” and, for mission-related tasks and exercises, a “mission cloud.” The Bundeswehr Centre for Software Expertise makes a crucial contribution in this field.

Harnessing Artificial Intelligence

The work of the Bundeswehr Centre for Software Expertise has already made it clear that the Cyber and Information Domain Service also places great value on exploiting the opportunities offered by digitalization. This also applies to the use of artificial intelligence (AI). For digitalization, AI presents a quantum leap – just as the assembly line did for industrialization. Weak AI—which, in contrast to strong AI, is limited to solving specific user problems—will become an integral part of our everyday lives, a tool that will assist us around the clock. This technology has enormous potential, particularly when it comes to structuring large amounts of data because, like a kind of metal detector, AI tools can find the proverbial needle in the haystack of big data.

A possible military application can be found, for instance, in early crisis detection. For this purpose, the Federal Ministry of Defence has been developing, in cooperation with industry, an IT support project for early crisis detection since 2017. Participants in the project include the Bundeswehr University in Munich. The above-mentioned Joint Cyber and Information Domain Fusion Centre of the Cyber and Information Domain Service will also employ AI tools in future in order to speed up decision-making and put it on a sounder basis. Here the immense advantage of AI becomes apparent. It relieves the analysts so that they can concentrate on what machines cannot do, i.e. drawing conclusions and deriving and assessing options for action. Here we touch on an issue that I regard as extremely

important: The decision about what to do with the information must and will always be made by human beings.

In the areas of Bundeswehr training, materiel maintenance, and logistics too, AI will certainly bring improvements in the future. The Army, for instance, is currently identifying possible uses of AI and machine learning techniques and implementing them as part of prototype projects. The Air Force is investigating the potential of employing AI in the Air Command and Control (AirC2) planning process and the use of AI in mission planning. In the medical field, imaging analysis is already being used in diagnostics.

It is, however, not only the Bundeswehr that has realized the military potential of AI; other nations are also stepping up research. Thus, the use of AI for military purposes is a topic of strategic importance.

Digital Networking on the Battlefield

My organizational element is responsible for the operation, use, protection, and further development of the Bundeswehr IT system. This ranges from office communication equipment, the provision of which is in the hands of the federally owned BWI company, to Bundeswehr weapon systems interfaces – from the Eurofighter system support equipment to the Navy's seaborne operations centre and the tablet computer of the infantry soldier on the battlefield. My objective is to provide the armed forces with the required IT services in an efficient and secure way. Here, particular attention is paid to the design of the overall system in order to ensure seamless transitions and interoperability, both internally and with external partners such as allied armed forces or other government agencies.

The Cyber and Information Domain Service plays a key role in the digitalization of the armed forces. It acts as the central armed forces requesting authority for IT projects. The Digitalization of Land-Based Operations (D-LBO) programme is a prominent example. This project is not only aimed at replacing the old SEM and TETRAPOL radio sets with IP-based services, but at the digital interconnection of all soldiers and vehicles on the battlefield as part of a mobile and seamless, nationally and multinationally interoperable network. It is intended that this will be guaranteed even in national and collective defence operations, which are characterized by frequent command post relocations and mobile conduct of operations. Modernizing the IT equipment of tens of thousands of vehicles and personnel is a mammoth project that will take several years to complete. The D-LBO programme is the key to the modernization of mobile information supply during operations.

Multinational and Whole-of-Government Approach

Multinationality has already been mentioned as an important guiding principle. It applies to the networking of systems and actors of different levels of command on the battlefield just as much as, in a very practical form, to the numerous NATO, EU, and binational exercises. In 2019, the Cyber and Information Domain Service again took part in the world's largest international live-fire cyber defence exercise, the NATO exercise *Locked Shields*. The Bundeswehr computer forensics

experts were chosen as the best team in their category for the fourth time in a row.

At the military-strategic level, too, we maintain close contact with our partners. Thus, while only in the second year of our existence, we were given the chairmanship of the Cyber Commanders Forum for one year. This body regularly brings together the cyber commanders of several NATO and non-NATO nations in order to strengthen multinational cooperation.

Furthermore, thanks to our cooperation with other national institutions, the Cyber and Information Domain Service also contributes to national security and strengthens Germany's cybersecurity architecture. For instance, close cooperation has developed with other security agencies, such as the Federal Office for Information Security. In our eyes, the development of the National Cyber Response Centre, which is subordinate to the Federal Office for Information Security, into an inter-ministerial and operational-level institution is essential for Germany's future capacity to act. With our expertise, we contribute to this process and address the issues, wherever possible, maintaining close contact with all parties involved.

In addition, we have agreed on first cooperation projects with the business and science sector, for instance with the German Telekom company, with the Fraunhofer Institute for Communication, Information Processing, and Ergonomics (FKIE), and—our most recent cooperation since May 2019—with Bitkom, Germany's leading association for information technology, telecommunications, and new media. At the regional level, the Cyber and Information Domain Service is part of the Cyber Security Cluster Bonn, maintaining connections with business companies, educational institutions, and government agencies in order to share information and best practices. This is achieved, for instance, through mutual job shadowing or the opening and support of training measures.

Personnel and Materiel

Suitably qualified and motivated personnel is increasingly becoming a strategic resource. Like many organizations and companies, the Bundeswehr faces the challenge of recruiting young talents in the field of cyber and information technology. From conversations with potential employees, we have learned that the Bundeswehr, with its specific task portfolio, is definitely an attractive employer for this target group. We use this as an advantage and offer incentives, for instance, by promoting education and training measures for our members. In January 2018, an international Master's degree programme in cybersecurity was launched at the Bundeswehr University in Munich. There, we are also creating a research centre for computer science and cybersecurity, which is unique in Germany.

As Chief of the Cyber and Information Domain Service, I fulfil the same role as the chiefs of staff of the other services when it comes to developing personnel requirements for the career paths that fall into my responsibility, i.e. cyber and information technology, military intelligence, operational communication, and geoinformation. This means that I have the lead responsibility for the design of

these predominantly technical career paths. For these careers, we will establish a holistic view on personnel issues across all major organizational areas and thus improve the existing range of individual professional perspectives.

Currently, we are also developing possibilities to take informal cyber and IT expertise of potential employees into stronger consideration, which will allow us to make attractive offers to these applicants, too. In addition, we have made significant progress when it comes to personnel augmentation by reservists and lateral entry employees. With more than 800 individuals interested in working for the cyber reserve and over 1400 users of the cyber community platform, a Bundeswehr virtual forum, the Cyber and Information Domain Service also benefits from external expertise. Furthermore, we are creating various flexible working opportunities and attempting to provide financial incentives, for instance, in the form of bonus payments for urgently needed IT specialists.

Regarding the issue of materiel, it is my wish to further streamline procurement and maintenance processes. Given the rapid development cycles in the cyber and IT sector, this is the only way we can ensure adequate equipment and maintenance. Numerous defence projects already exist that contribute to the modernization of C2 capability in the Bundeswehr. Above, I have described in detail how the Cyber and Information Domain Service contributes to this through the digitalization of land-based systems.

International Law

In general, the use of military cyber capabilities is subject to the same constraints under international and constitutional law that apply to any other operation of the German armed forces. At the international level, there also exists a definitive but non-binding regulation on how to apply existing international law to cyber operations, the Tallinn Manual 2.0.³ These legal and ethical foundations are to be taken into account for all measures in cyber and information space. So, although the foundations of legal security have been laid down, there is still much to be done in this area. Indeed, it is indisputable—and has by now become consensus—that the binding international rules that govern armed conflict between states must also be applied to the cyber and information domain. Therefore, in order to allow a quick response to attacks if necessary, the issue of how these rules are to be applied to this new domain must be considered in detail.

The Way Forward

The challenges in the cyber and information domain, which have been described above, will increase further, both in quality and in quantity. Therefore, adequate protection is vital for the state, the economy, and society. In Germany, this is regarded as a national task, which is to be approached together with international partners.

³ Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017).

This is also how the most recent major organizational element of the Bundeswehr sees itself. The Cyber and Information Domain Service is responsible for the Bundeswehr IT system as well as for reconnaissance, effects, and geoinformation. During routine duty, operations, and exercises, it closely cooperates with other parts of the Bundeswehr as well as with friendly armed forces and other national authorities.

With respect to digitalization in the Bundeswehr, it is important not only to counter the risks but also, and especially, to exploit the inherent opportunities. This largely applies to technical aspects. At the same time, however, a new way of thinking is required when it comes to operations in cyber and information space. Cyber and information domain operations constitute an independent field of operations and provide support to land, air, and maritime missions as part of conventional military operations. Therefore, in order to provide politicians with non-kinetic options, these capabilities must be developed across the entire spectrum of cyber and information domain operations.

The government must maintain its capability to act and to ensure the protection of the people and the provision of basic services. Here, the capabilities of the Bundeswehr in the cyber and information domain can make a vital contribution.

Disclaimer

The views expressed are solely those of the contributing authors and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

About the Author

Lieutenant General **Ludwig Leinhos** joined the Bundeswehr as Air Force officer candidate in 1975. His studies of electrical engineering and graduation as Diplom-Ingenieur at the Bundeswehr University Munich were followed by training and assignments in the field of electronic warfare. From 1988 until 1990 he attended the General Staff Officer Course at the Bundeswehr Command and Staff College in Hamburg.

His subsequent military career was characterized by various ministerial staff and leadership assignments in Germany and abroad in the fields of command and control systems, signals intelligence, as well as IT planning and application. As General Manager at NAPMA, he was responsible for the program management organization of NATO's AWACS fleet. From 2013 until 2016, he was in charge of cyber defence and numerous IT standardization issues, among others, as Director, NATO Headquarters C3 Staff at NATO Headquarters in Brussels.

From 2016 onwards, Lieutenant General Leinhos as Director, Activation Staff of the German Cyber and Information Domain Service has set the course for the new Service of the Bundeswehr, and on 1 April 2017 became the first Chief of the German Cyber and Information Domain Service.



Austria's National Cyber Security and Defense Policy: Challenges and the Way Forward

Major General Hermann Kaponig

ICT & Cyber Security Center, Austrian Armed Forces

Abstract: The article presents Austria's cybersecurity policy, set in a whole-of-government context. It is comprehensive, integrated, proactive, and based on solidarity and cooperation within and beyond the European Union. Transparent governance, the cooperation between public agencies, businesses, research institutes, and the citizens, investments in awareness, research and development are expected to protect effectively vital information and critical infrastructures. The Ministry of Defense and the Austrian Armed Forces contribute to the national policy primarily through the Joint Forces Command, the Communication and Information Systems & Cyber Defense Command, and the two intelligence services.

Keywords: cyber defense, critical infrastructure, whole-of-government, interagency cooperation, cybersecurity platform.

Policy Highlights: Austria's National Military Cyber Defense Policy Within a Whole-of-Government Context

The "Austrian Security Strategy: Security for a New Decade – Shaping Security," adopted by the Austrian National Council in 2013 (ÖSS 2013)¹ was followed in the same year by the "Austrian Cyber Security Strategy" (ÖSCS 2013),² which was

¹ "Österreichische Sicherheitsstrategie: Sicherheit in einer neuen Dekade – Sicherheit gestalten," Vienna, July 2013, https://www.bmi.gv.at/502/files/130717_Sicherheitsstrategie_Kern_A4_WEB_barrierefrei.pdf.

² "Austrian Cyber Security Strategy," Vienna, 2013, https://www.bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf.

produced in accordance with the ÖSS. Both documents were developed at the national level.

The ÖSS 2013 describes new challenges, risks, and threats, including cyber threats (attacks against the security of IT systems, or “cyberattacks”) based on analysis of the Austrian security environment. In addition, the ÖSS 2013 distinguishes between two key areas in terms of required policy development.

The chapter “Security policy at the national level: *Internal security*” discusses cybercrime, cyberattacks, and the misuse of the Internet for extremist purposes as well as network security posing new and specific challenges for all actors concerned. Moreover, this chapter points out that *broad cooperation based on a comprehensive concept* is required. In the same chapter, under “*Defense policy*,” it posits that managing sub-conventional threats and new hazards resulting from cyberattacks may create a new area of military activity. From these two subchapters, one can infer that the ÖSS recognizes modern cyber threats but does not elaborate explicit countermeasures.

The military is required to expand its cyber capabilities following the national cybersecurity concept. This means that the military must be capable of providing cyber support and assistance comparable to military assistance in the case of disaster relief.

On 3 July 2013, the National Council passed a resolution requesting that the Federal Government develop Austria’s security policy along with certain principles. The guideline for cybersecurity states:

Threats caused by state and non-state actors in cyberspace are constantly on the rise. This is why cybersecurity is becoming more and more important. Measures to increase the security of computer systems, as well as Internet security, shall be intensified.

The Austrian Cyber Security Strategy of 2013 must be implemented and updated regularly following current developments. This means that the ÖSCS 2013 is to be implemented at the national level and developed further. Currently, national plans for an ÖSCS 2.0—which will be based on already accomplished ÖSCS 2013 objectives as well as developments and requirements that have occurred since then—are being developed.

The introduction to the ÖSCS 2013 explains that attacks from cyberspace pose a direct threat to the safety and the proper functioning of the state, the economy, science, and society. They can have a profound negative impact on our daily lives. Non-state actors like criminals, organized crime, or terrorists, as well as state actors like secret services and the military, may misuse cyberspace for their purposes and interfere with its proper functioning. Both the threats in cyberspace and the productive use thereof are practically infinite. It is, therefore, *Austria’s top priority to work towards securing cyberspace at the national and international levels*. Cybersecurity means the security of cyberspace infrastructure, the security of data exchange in cyberspace, and above all, the protection of the people using cyberspace.

It is a joint, core task of the state, the economy, and society to ensure cybersecurity nationally and internationally. The ÖSCS 2013 is a comprehensive and proactive concept for protecting cyberspace and the people in cyberspace while guaranteeing human rights. The strategy is expected to contribute to the security and resilience of Austrian infrastructures and services in cyberspace. Most importantly, it will build awareness and confidence in Austrian society.

The chapter on “Risks and threats” states that cyberspace and the security and safety of people in cyberspace are exposed to a number of risks and threats since cyberspace is also a space of criminal activity. Risks and threats span the spectrum from operating errors to massive attacks by state actors and non-state groups using cyberspace as operational fora not limited by national borders. *Foreign military organizations may also be behind these attacks.*

The spectrum of risks and threats was presented in a specific Cyber Risk Matrix (effective 2011).³ The Risk Matrix was revised and updated in 2016.⁴ Cyber-crime, identity fraud, cyberattacks, or misuse of the Internet for extremist purposes are new serious challenges that require broad cooperation between governmental and non-governmental agencies at the national and international levels. This is a clear indication that countering cyber challenges is a top priority on the national agenda and that all forces need to join in a whole-of-government cooperative approach, and that national and international cooperation and interaction are essential.

The chapter on “Principles” continues with the following definitions:

State-of-the-art cybersecurity policy is a cross-cutting issue that impacts many spheres of life and policy. It must be developed in terms of a comprehensive and integrated approach, to allow for active participation and has to be implemented in the spirit of solidarity.

Comprehensive cybersecurity policy means that external and internal security, as well as aspects of civilian and military security, are closely interlinked. Cybersecurity goes beyond the purview of traditional security authorities and comprises instruments of numerous policy areas.

Integrated cybersecurity policy emphasizes task-sharing between the state, economy, academia, and civil society. It comprises measures in the following areas: political-strategic control, education and training, risk assessment, prevention and preparedness, detection and response, mitigation and restoration, as well as the development of governmental and non-governmental capabilities and capacities. An integrated cybersecurity policy must be based on a cooperative approach both at national and international levels.

Proactive cybersecurity policy means that efforts are made to prevent threats to cyberspace and the people in cyberspace as well as to mitigate the impact of incidents (shaping security).

³ “Cyber-Risikomatrix 2011,” https://kuratorium-sicheres-oesterreich.at/wp-content/uploads/2015/02/KSO_Cyber_Risikomatrix.pdf, accessed March 12, 2020.

⁴ “Cyber-Risikomatrix 2011.”

Cybersecurity policy based on solidarity takes into account that due to the global nature of cyberspace today, the cybersecurity of Austria, the EU, and the entire community of nations is strongly interconnected. Ensuring cybersecurity requires intensive cooperation based on solidarity at European and international levels.

Austria's Main Policy Challenges and Key Priority Areas

Based on strategic objectives, the ÖSCS 2013 identifies seven fields of action and a total of 15 measures:

- Field of action 1 – Structures and processes
- Field of action 2 – Governance
- Field of action 3 – Cooperation of government, economy, and society
- Field of action 4 – Critical infrastructure protection
- Field of action 5 – Awareness-raising and training
- Field of action 6 – Research and development
- Field of action 7 – International cooperation.

Field of Action 1 – Structures and Processes

Objective: There are numerous structures and stakeholders active in cyberspace that are working separately from each other to ensure cybersecurity. Several organizations specializing in cybersecurity (e.g., Computer Emergency Response Teams, CERTs) are already playing an important role in cyber crisis management. Overarching cybersecurity procedures have not been defined formally so far. Therefore, it is necessary to define processes and structures to provide for overall coordination at the political-strategic level, as well as at the operational level by involving all relevant public and private stakeholders.

Measures:

1) Establishing a Cyber Security Steering Group

In 2012, the Austrian Council of Ministers formed a *Cyber Security Steering Group*. Under the leadership of the Federal Chancellery, the group is responsible for coordinating measures related to cybersecurity at the political-strategic level, monitoring and supporting the implementation of the ÖSCS 2013, drafting an annual Cyber Security Report, and advising the federal government in all matters relating to cybersecurity. The Steering Group includes liaison officers working with the National Security Council and cybersecurity experts from the ministries represented in the National Security Council. The Chief Information Officer of the Federal Republic of Austria (National CIO) is also a member of this body. In case of specific issues, representatives of other ministries and the Austrian federal provinces may be included in the Steering Group as required. This holds especially for agencies dealing with organizations and enterprises that are subject

to or affected by control measures. Representatives of other relevant enterprises become included on an appropriate, case-specific basis.

2) Creating a structure for coordination at the operational level

An *Operational Coordination Structure* will be created on the basis of existing operational structures to serve as a platform for preparing incident-related and periodic cybersecurity reports and for deliberations on measures to be taken at the operational level. Thus, it will provide a continuously updated overview of cyber developments by collecting, compiling, evaluating, and passing on relevant information. The economic sector should be involved in an appropriate manner and on an equal footing. The joint and permanently updated overview report will indicate the current cyber status and serve as a basis for planning preventive and response measures. The operators of critical infrastructure will be supported at the operational level and particularly in cases of failures of information and communication structures. Besides, they will be provided with information on dangers to the Internet. The Operational Coordination Structure must be designed so that it can be used as an operational executive body of cyber crisis management leaders.

The *Operational Coordination Structure* engages ministries and operational structures of business and research sectors. The tasks performed within the Operational Coordination Structure are coordinated by the Federal Ministry of the Interior (in a public-private partnership, or PPP arrangement). In carrying out its coordination task, the Federal Ministry of the Interior (BMI) is supported by the Federal Ministry of Defense (BMLV), to which coordination tasks will be transferred if a cyber defense incident occurs. All operational, organizational, sectoral, or target group-specific structures will remain within the purview of the respective organization. Institutions with responsibilities for security issues of computer systems, the Internet, and the protection of critical infrastructure, will cooperate within the framework of the Operational Coordination Structure. At the national level, these organizations comprise the GovCERT (Government Computer Emergency Response Team), MilCERT (Military Computer Emergency Readiness Team), and the Cyber Crime Competence Center (C4). Other government institutions are involved by forming a second circle. The additional circle comprises private CERTs (CERT.at, BRZ-CERT, banks, etc.), as well as economic sectors and research institutes.

The Cyber Security Steering Group will establish a *working group* in charge of preparing proposals for necessary processes and structures for permanent coordination at the operational level. Representatives of relevant enterprises will be involved appropriately.

3) Establishing a Cyber Crisis Management system

Austria's *Cyber Crisis Management* consists of state representatives and operators of critical infrastructure. In terms of composition and working procedures, it is modeled on the National Crisis and Civil Protection Management (Austrian

abbreviation: SKKM) arrangements. Since its responsibilities go beyond information and communications technology (ICT) and to ensure internal security in case of overarching threats, the Federal Ministry of the Interior will be responsible for cyber crisis management coordination. As far as external security is concerned, the Federal Ministry of Defense will play the leading role in coordinating measures to protect sovereignty by ensuring national defense (cyber defense). *Crisis management and continuity plans* will be prepared and updated regularly in cooperation with public institutions and the operators of critical infrastructure based on risk analyses for sector-specific and cross-sectoral cyber threats.

Further, *regular cyber exercises* will be held to test Austria's Cyber Crisis Management System as well as crisis and continuity plans.

4) *Strengthening of existing cyber structures*

The role of the *GovCERT* operated by the Federal Chancellery as the government's CERT will be strengthened. Towards that purpose, it will be necessary to describe in detail its powers, responsibilities, and spheres of action, its institutional place within the public administration, role in the event of a crisis, and the modalities of interaction with the Operational Coordination Structure. Further, new requirements will have to be defined.

To avoid and prevent cybercrime as well as to facilitate operational international cooperation, the role of the *Cyber Crime Competence Center (C4)* of the Federal Ministry of the Interior will be enhanced. This Center is Austria's central body in charge of exercising security and criminal police duties in the area of cybersecurity.

The *MilCERT*, operated by the Federal Ministry of Defense, will be expanded to provide operational capabilities for preventing cyberattacks, to protect its own networks, and to further develop the Cyber Security Overview. These capabilities will, inter alia, also lead to the creation of capacity for providing ICT assistance to other state agencies.

The Austrian *CERT Association* will be enlarged, and *CERT.at* strengthened to facilitate national cooperation among Austrian CERTs. On the one hand, this will help to promote the establishment of CERTs in all sectors and, on the other, will intensify the exchange of information and experience on CERT-specific issues.

Field of Action 2 – Governance

Objective: The aim concerning governance is to define the role, responsibilities, and powers of state and non-state actors in cyberspace and to create adequate framework conditions for cooperation among all players.

Measures:

5) *Establishing a modern regulatory framework*

With the support of the *Cyber Security Steering Group*, a comprehensive report analyzing the need to establish additional *legal principles, regulatory measures, and voluntary self-commitment* (codes of conduct) for guaranteeing cyber secu-

ity in Austria will be prepared and submitted to the Federal Government. This report will cover the following issues: the establishment of necessary organizational structures, tasks and powers of authorities, information exchange between authorities and private entities, reporting duties, obligation to adopt protective measures as well as supply chain security.

Balancing incentives and sanctions should be considered when determining obligations for non-state actors.

6) Defining minimum standards

All relevant stakeholders should cooperate and define *minimum security standards* in order to ensure effective prevention and to achieve a common understanding of current requirements. These requirements will be applied to all components and services used in all security-relevant ICT areas. The applicable norms, standards, codes of conduct, and best practices, will be compiled in the *Austrian Information Security Management Handbook*, which will be updated regularly.

7) Preparing an annual report on cybersecurity

The Cyber Security Steering Group will prepare an annual report entitled “Cyber Security in Austria.”

Field of Action 3 – Cooperation of Government, Economy, and Society

Objective: Many tasks and responsibilities of public administration agencies, economic entities, and the world at large are based on the information and communications technology (ICT). The responsibility of using digital technologies in a prudent way rests with each organizational unit. However, it is only a broad cooperation between all sectors and permanent exchange of information that will facilitate the transparent and safe use of ICT. Therefore, existing cyber capacities and processes in the administration, the economy and within the population must be strengthened and new opportunities must be created through cooperation.

Measures:

8) Establishing a Cybersecurity Platform

The *Austrian Cyber Security Platform* will be operated as a public-private partnership to facilitate ongoing communication with all stakeholders of the administration, economy, and academia. In parallel, existing initiatives (run by the Austrian Trust Circle, Cyber Security Austria, the Austrian independent non-profit security association *Kuratorium Sicheres Österreich* (KSÖ), the Austrian Center for Secure Information Technology (A-SIT), etc.) will be continued and leveraged. The Austrian Cyber Security Platform will serve as the institutional framework for continuous exchange of information within the public administration and between the administration and representatives of the business, academia, and

research institutes. All will participate on an equal footing in the Cyber Security Platform, advising and supporting the Cyber Security Steering Group.

Cooperation with private operators of critical infrastructure and other economic sectors is essential for Austria's cybersecurity. Details on this cooperation will be discussed in further talks between the Cyber Security Steering Group and the economic sector.

The Cyber Security Platform will be used to initiate extensive *cooperation between the participating partners* on issues like awareness-raising and training as well as research and development.

In order to promote a common understanding of challenges and opportunities for action among all partners involved in cybersecurity issues, an *exchange* of experts should be intensified between the participating governmental, private, and academic organizations. Under the leadership of the Cyber Security Steering Group and with the support of the Austrian Cyber Security Platform, a program will be developed for this purpose.

9) Strengthening support for small and medium-sized enterprises (SMEs)

Priority programs on cybersecurity will be launched to raise cybersecurity awareness among SMEs and to prepare them for hazardous situations. Interest groups should be encouraged to post tailored information for SME needs online on the new Internet portal, ICT Security, and to initiate cybersecurity campaigns for SMEs. Support by governmental bodies, sector-specific information platforms such as the Austrian Trust Circles will develop sector-specific cyber risk management plans. Regulatory authorities and interest representations should be involved in this dialog. These risk management plans will be harmonized with governmental crisis and continuity management plans. Cross-sectoral cyber exercises for SMEs will be organized and held at periodic intervals. SME sectors should also be allowed to participate in governmental cross-sectoral cyber exercises upon request.

10) Preparing a Cyber Security Communication Strategy

In order to optimize communication between stakeholders in the administration, economy, academia, and society, all existing and planned government websites must be harmonized as part of a *Cyber Security Communication Strategy*. This communication strategy will be prepared by the Cyber Security Steering Group and involve the input of all relevant stakeholders.

Field of Action 4 –Critical Infrastructure Protection

Objective: Almost all infrastructures increasingly depend on specialized ICT systems, which guarantee smooth, reliable, and continuous operations to the greatest possible extent. It is, therefore, a top priority to build and improve the threat resilience of information systems. Under the Austrian Program for Critical Infrastructure Protection (APCIP), enterprises operating critical infrastructure are urged to implement comprehensive security architectures. The ÖSCS aims to

supplement and intensify these measures in the field of cybersecurity. In this process, cooperation with operators of critical information infrastructures is of paramount importance.

Measures:

11) Improving the resilience of critical infrastructure

The operators of critical infrastructure should be involved in all processes of national cyber crisis management. These strategic enterprises are tasked to define a comprehensive security (risk and crisis management) architecture, update it according to current threats, appoint a security officer, and further prepare for *crisis communication*. Also, *cybersecurity standards* should be set up for these enterprises and implemented in a partnership approach.

The operators of critical infrastructure should have a duty to report *severe cyber incidents*. The appropriate legal basis must be established after comprehensive consultations with the relevant stakeholders.

Existing arrangements in the *Program for Critical Infrastructure Protection* (APCIP) and the *National Crisis and Civil Protection Management* (SKKM) should be reviewed on an ongoing basis to ensure the continuous countering of new cyber challenges and to effect modifications if required.

Field of Action 5 – Awareness-Raising and Training

Objective: All target groups should be sensitized to cybersecurity in order to increase the awareness of, personal interest in, and the attention paid to it. These awareness-raising measures will help create an understanding of the need to ensure cybersecurity. Concrete and target-group-specific measures will impart and promote the necessary knowledge about security-conscious behavior and responsible use of information and ICT tools at large. Increased training in cybersecurity and media literacy in schools and other educational facilities, as well as adding cybersecurity competence to teaching, should ensure a meaningful and adequate level of ICT competence level across the board.

Measures:

12) Strengthening a cybersecurity culture

Awareness-raising initiatives are developed, coordinated, and implemented in harmony with a common approach whilst taking into account existing programs. In doing so, it is important to examine cybersecurity from different perspectives, highlight relevant dangers, draw attention to possible impacts and damages as well as make recommendations for security measures.

In order to give different target groups access to more in-depth customized advice, the existing *consulting programs* should be further enhanced and expanded.

A web-based *ICT Security Internet Portal* will be set up to serve as an information and communication hub for awareness-raising. The Ministry of Finance,

the Federal Chancellery, and A-SIT will be responsible for coordinating the ICT Security Internet Portal. The strategic approach of this portal will be guided by the principles and objectives of the ÖSCS.

Prevention programs safeguarding against cybercrime will be further developed.

13) Incorporating cybersecurity and media literacy into all levels of education and training

Austria will pursue stronger integration of ICT, cybersecurity, and media literacy into *school curricula*. ICT and new media literacy are part of the curriculum of all types of schools. ICT security issues and cybersecurity will eventually become an integral part of a model called *Digital Competence*. This model will be adjusted to the curriculum of the respective type of school and will create awareness for security issues and promote the safe and responsible use of the Internet. The aim is to ensure a certain level of ICT competence across all types of schools.

ICT (security) competence should be part of *academic training* at pedagogical universities as well as pedagogical institutes of higher education. Teachers will need to receive cyber education before they can teach cyber skills at the secondary school level as well as at adult education centers.

The *training of public sector experts* responsible for improving cybersecurity will be intensified in cooperation with national and international training facilities.

ICT system administrators working for operators of critical infrastructure should receive additional cybersecurity training in order to be able to recognize cyber incidents, detect anomalies in their ICT systems and report them to their security officers (*Human Sensor Program*).

Field of Action 6 – Research and Development

Objective: To ensure cybersecurity technical expertise, based on state-of-the-art research and development results. To this end, cybersecurity issues must be increasingly incorporated into applied cyber research as well as into security research programs such as the Austrian KIRAS program. Efforts should be invested to achieve active thematic leadership in EU security research programs.

Measures:

14) Strengthening Austria's cybersecurity research

Within the scope of national and EU security research programs, *cybersecurity* should be a *key research priority*. Through joint projects, relevant stakeholders from the administration, business, and research organizations will develop the conceptual framework and technological instruments to enhance Austria's cybersecurity capacity. Particular emphasis will be placed on measures helping to turn research and development findings speedily into marketable products. Existing research projects, such as those run by A-SIT, will be further developed.

Austria should strive for *active thematic leadership in EU security research programs*. In doing so, Austria should initiate the incorporation of cyber topics that are important for Austria into international research programs.

Field of Action 7 – International Cooperation

Objective: Global networking and international cooperation are vital factors in ÖSCS. Security in cyberspace can be achieved only through a coordinated policy mix at the national and international levels. Therefore, Austria will engage in an active cyber foreign policy and pursue its interests in a coordinated and targeted way within the framework of the EU, UN, OSCE, Council of Europe, OECD, and NATO partnerships. Furthermore, the international aspects of Austria's cyber policy will be harmonized consistently in other policy fields.

Measures:

15) Effective collaboration on cybersecurity in Europe and worldwide

Austria will make a substantial contribution to the development and implementation of the *EU Cyber Security Strategy*. It will participate fully in the strategic and operational work of the EU.

The relevant ministries will take the necessary measures to implement and to make full use of the *Convention on Cybercrime* of the Council of Europe.

Austria advocates for a free Internet at the international level, which will guarantee the free exercise of all *human rights in the virtual space*. In particular, the right to freedom of expression and information must not be restricted on the Internet without legal cause. This is the position that Austria shall adopt in international forums. Hence, Austria will participate actively in developing and establishing a transnational code of conduct for government activity in cyberspace, which will also include measures to build confidence and security.

Austria will continue its bilateral cooperation, initiated within the framework of NATO Partnership for Peace, and actively support the preparation of a list of concrete confidence and security-building measures in the framework of the OSCE.

Austria already participates actively in planning and implementing *transnational cyber exercises*. The experience gained from such exercises will be used as a direct input for planning and further developing operational cooperation.

Foreign policy measures that pertain to cybersecurity are coordinated by the Federal Ministry of Europe, Integration and Foreign Affairs (BMEIA). Where appropriate, the conclusion of bilateral or international agreements will be taken into consideration.

Implementing Policy Structures Within a Whole-of-Nation Context

In Austria, the coordinating structures for managing cyber challenges are as follows. At the highest level, which is the *political level*, the Austrian government defines its political and strategic objectives. The *National Security Council (NSR)*

functions as the national security advisory body at the *strategic level*. In case of a cyber incident, the NSR will draw on the *Cyber Security Steering Group (CSSG)*. The CSSG coordinates cybersecurity measures at the political-strategic level under the leadership of the Federal Chancellery. It also monitors and supports the implementation of the ÖSCS, produces an annual report on cybersecurity and advises the federal government on cybersecurity issues.

The *Cyber Security Platform (CSP)* will also provide support in case of a cyber incident. The CSP is the primary platform for cooperation and exchange of information between business, science, research, critical infrastructure, and public administration entities.

Depending on the type of cybersecurity threat, it will be either the *Inner Circle of Operational Coordination (IKDOK)* or the *Extended Circle of Operational Coordination (EKDOK)* that will be tasked at the *operational level*.

The IKDOK is responsible for operational control and coordination in the area of cyber. It maintains contact with the operators of critical infrastructure, businesses, and ministry departments working in cyber and develops standards and operational measures to be implemented in case of a cyber crisis incident. The IKDOK also serves as an interagency platform for information exchange. It develops an intermittent incident-related Cyber Security Overview Report and discusses necessary operational measures. It provides a continuously updated overview of cyber developments by collecting, compiling, evaluating, and passing on relevant information. The IKDOK is comprised of representatives of the Federal Chancellery, the Ministry of the Interior (Mol), the MoD, and the BMEIA and also



Figure 1: Permanent Operative Coordination Structure.

includes the Cyber Security Center (CSC; MoI) and the Cyber Defense Center (CDC; MoD), both of which chair the IKDOK, and involves other state actors/agencies as well. This means that all cyber assets in the national cyber community are included in the IKDOK: the CSC and the C4 of the MoI; the CDC and MilCert of the MoD; the GovCERT; etc.

As far as the *GovCert* is concerned, it is the superstructure of all state CERTs and plays a leading role in public administration.

The *EKDOK* is essentially the extended circle of IKDOK plus the CERT Association. The *CERT Association* enhances CERT structures at the national level. It intensifies cooperative efforts with sector-specific CERTs (engaging in defined critical infrastructure sectors).

At the national level, there are also civilian agencies with similar setups working alongside state CERTs. They serve first and foremost as crisis intervention teams in cases of cyberattacks against civilian companies or business sectors. These civilian agencies are organized in groups along sector-specific lines. The CERT.at serves as their superstructure and, in cooperation with the Federal Chancellery, has established the Austrian Trust Circle. The Austrian Trust Circle offers a formal framework for security information exchange between the CERT.at, the Federal Chancellery, and the GovCERT. Within the framework of this partnership, it is foreseen to link all Austrian CERTs to discuss standards, provide assistance to affected companies and business sectors, and to develop joint strategies in the event of a cyberattack.

Core Responsibilities

The MoI is responsible for *cybercrime* and the *protection of critical infrastructure*.

The MoD is primarily responsible for *cyber defense* and its three subcomponents: *cyber intelligence* (under the purview of the Armed Forces Protection Service and the Armed Forces Intelligence Service), *ICT security* (under the purview of the ICT & Cyber Security Center) and *cyber operations* (under the purview of the Armed Forces Command). In addition, in cases of cyber incidents, military forces will provide assistance to support the overall mission.

The BMEIA is responsible for *cyber diplomacy*.

Responsibilities during Cyber Incidents

Austria distinguishes between *three cyber threat levels* determined by the degree of cyber risk escalation.

The first level pertains to *cyber standard operations*, where cybercrime, cyber espionage, and data theft must be managed appropriately. At this level, the MoI is responsible for response coordination. The MoI coordinates the close cooperation, exchange of information and mutual support between all stakeholders taking advantage of the IKDOK. The MoD must be able to take appropriate action within its scope of responsibilities and, as necessary, support other public institutions upon request for assistance.

The second level pertains to *cyber crisis* when incidents ranging from cyberattacks on critical infrastructure to blackouts caused by cyberattacks have to be

managed appropriately. At this level, it is also the MoI that is responsible for response coordination. The MoI coordinates close cooperation, exchange of information, and, if necessary, mutual assistance between all stakeholders. At the strategic level, the Cyber Security Steering Group will be activated and will take charge of the IKDOK and the CSC of the MoI. Again, the MoD must be able to take appropriate action within its scope of responsibilities and, if necessary, support other agencies upon request for assistance.

The third level pertains to *cyber defense* when politically motivated attacks pose a substantial threat to state sovereignty. In this case, response coordination is transferred to the MoD. At the strategic level, the Cyber Security Steering Group will be activated and will take charge of the IKDOK and use the CDC of the MoD for action at the operational level. The MoD will coordinate the close cooperation, exchange of information, and, if necessary, mutual support between all stakeholders.

It must be noted that the systematic transfer of authority from the MoI to the MoD cannot be effected categorically or preplanned in detail in the case of cyber crisis turning into cyber defense. A checklist was developed at the national level, which defines the preconditions for such a transfer. During an actual cyber incident, however, the transfer of authority will have to be determined based on a thorough situational assessment.

Policy Implementation in the Austrian MoD and Armed Forces

The ÖSCS 2013 has tasked the Federal Ministry of Defense (BMLVS) with performing important missions and measures. Also, the Ministry of Defense (MoD) is bound by the Defense Strategy 2014 (TV14) as well as by the Military Strategy 2017 (MSK17). Up to now, the MoD has worked with its existing concept papers. Currently, the MoD is developing a Cyber Defense Strategy (CDS) and a Concept for Military Cyber Operations (CyOps).

The national defense structural reform (LV21.1) of 2016 created the “Communication and Information Systems & Cyber Defense Command” (CIS & CD Command; KdoFüU&CD), which was a separate military branch exercising operational leadership and cyber capabilities. In doing so, almost all capabilities in the area of leadership support, ICT, electronic warfare, cyber defense, and navigation operations were packed into one command.

Due to budgetary reasons, this ambitious goal had to be abandoned, and in 2019 the CIS & CD Command was ultimately dissolved. The following military structures now exercise the responsibilities for merely cyber defense:

- The Joint Forces Command (JFC) is responsible for Cyber Operations (CyOps).
- The CIS & Cyber Security Center (CISDC) is responsible for ICT defense.
- The two military intelligence services—the Armed Forces Security Agency (AFSA) and the Austrian Strategic Intelligence Agency (ASIA)—are responsible for the subdomain of cyber intelligence (CyInt).

Austrian military cyber defense focuses on network protection and will be expanded following medium and long-term armed forces' development goals.

Austria's Key National Initiatives and Policy Response Challenges

Currently, the main challenge is the full implementation at the national level of policies based on EU-wide legislation on cybersecurity known as the Directive on security of network and information systems (NIS Directive). This will set the course for increasing network and information system security in the long-term. Above all, it will enhance the security of particular critical infrastructures in various sectors.

Beyond this, as mentioned above, a new whole-of-nation Austrian Cyber Security Strategy is currently being developed at the national level.

Further, cooperative efforts are being intensified at all levels. On the one hand, cooperation at the national level between public and private business entities as well as cooperation between the military and the civilian sector is being strengthened. On the other hand, cooperative efforts between Austria and international organizations like NATO and the EU are being reinforced. As far as the EU is concerned, Permanent Structure Cooperation (PESCO) projects are also being initiated in the cyber area.

The Austrian Armed Forces (Österreichisches Bundesheer) also take advantage of the knowledge provided by the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE), a multinational and interdisciplinary cyber defense hub.

The Austrian Armed Forces also take part in joint international exercises to promote cyber capability development and cyber defense interoperability. Austria, Germany, and Switzerland belong to the trilateral cooperation of "D-A-CH" nations and hold interoperability exercises annually. Austria regularly participates in these exercises and also participated in the *Common Roof* 2018 interoperability exercise.

Austria regularly participates in major exercises such as *Locked Shields*, an international technical live-fire cyber defense exercise organized by the NATO CCDCOE, or the technically-oriented *KSÖ-Planspiele*, a cybersecurity simulation exercise organized nationally by the Kuratorium Sicheres Österreich (KSÖ), an Austrian independent non-profit association aiming at making Austria more secure), The Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX), a NATO interoperability event, Cyber.PHALANX 2018, an exercise designed for military planners and staff, and the Austrian Strategic Decision Making Exercise ASDEM18, to name just a few of the well-known exercises.

It is worth noticing that Austria is involved in a significant number of bilateral cooperative relations, primarily with other member states of the European Union, but is also engaging in a new cooperation with the Israel Defense Forces.

Moreover, every year Austria conducts the Austria Cyber Security Challenge, which is a contest to search nationally for talent. The winning team also represents Austria in the European Cyber Security Challenge.

Engaging the Austrian Private Sector and Academia

In the private sector, the research and technology activities of the Austrian Institute of Technology (AIT) and the work of the organization KSÖ are worth noting. In the academic sector, the Graz University of Technology and the Cybersecurity Campus Graz (a partnership between the Graz University of Technology and SGS), the Campus Hagenberg of the University of Applied Sciences Upper Austria and the St. Pölten University of Applied Sciences are worth noting.

Confronting Outstanding Limitations

The following limitations need to be considered in an Austrian context:

- The budgetary pressure on defense spending, which currently amounts to approximately 0.58% of the GDP.
- The legal framework, which currently allows for offensive cyber operations to be carried out only in incidents categorized as “national cyber defense.” According to current law, cyberattacks below the cyber defense threat level (at the level of “cyber standard operations” or “cyber crisis”) are not permitted.
- Recruiting cyber experts has become one of the most fundamental challenges. Currently, Austria’s educational infrastructure does not produce the required amount of specialists to cover demands in the public sector, the military, and the private business sector. As a result, there is fierce competition for the best experts. Nevertheless, thanks to the conscript system, the Austrian Armed Forces have a certain advantage over other public agencies and the economy, since trained cyber and ICT specialists are available to the military on a regular or temporary basis. These cyber recruits receive additional training during their military service and their expertise is put to good use. Also, the Austrian militia system includes cyber specialists that are called upon as cyber experts for military purposes.

As the next step in cyber education, Austria is considering establishing a separate military cyber & ICT training system. Developments towards cyber training, allowing for specialized career tracks for non-commissioned officers and officers, are underway. This will guarantee that the military can draw from its personnel to cover cyber and ICT expertise.

- It is a drawback in cyber defense that Austrian Armed Forces cyber experts are not part of the NATO Communications and Information Agency’s Malware Information Sharing Platform community.

The Way Forward

Due to significant developments in military cyber affairs, it would be expedient to go even beyond the current, already ambitious EU efforts (for instance led by the European Defense Agency, the European Union Agency for Cybersecurity ENISA (formerly, European Union Agency for Network and Information Security), and computer emergency response teams for the EU institutions, agencies, etc.) and set up a central cyber office or cyber cell in the European Union Military Staff. It would be more than expedient if EU member states could manage developments both in a top-down and bottom-up approach.

The current Austrian government program foresees the establishment of a National Cyber Security Center for Austria, thereby engaging all major state players. Such a center is considered essential and, once available and operable, it will significantly improve effectiveness, the flow of information, situational awareness analysis, and response speed.

It would certainly be helpful if the NATO CCDCOE were to expand its task portfolio and develop into a central hub for all levels of cyber affairs (strategic, operational, tactical/technical, research).

Furthermore, it would be advisable if, under EU leadership, Europe could trigger significant cyber developments including measures such as developing *cyber technology clusters* (e.g., determining which nation is positioning itself or taking the lead in which research area or in which cyber industry) and increasing the technical security of networks and establishing European *standards* for various engineering solutions to create a higher degree of security by design and artificial intelligence in future ICT, weapon and sensor systems from the outset.

Disclaimer

The views expressed are solely those of the contributing author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

About the Author

Brigadier **Hermann KAPONIG** is the cyber coordinator of the Austrian Ministry of defense. Previously, he has served as head of the Command Support Center of the Austrian Armed Forces, head of the MOD Logistics Directorate, and head of the Planning and Armaments Section in the Cabinet of the Federal Minister of Defense and Sports.



Responding to the Cyber Threat: A UK Military Perspective

*Air Commodore Phil Lester, Royal Air Force
and Captain Sean Moore, Royal Navy*

Abstract: The article reviews the UK military contribution to the national approach to cybersecurity, extending across the continuum of inter-state activity from peace, through cooperation, competition, confrontation, conflict, and war. According to the UK doctrine, the military performs active and passive defensive functions in cyberspace, offensive cyber operations, cyber intelligence, surveillance and reconnaissance, and cyber operational preparation of the environment, and the response actions are not limited to just the cyber domain.

Keywords: military cyber capabilities, cyber operations, strategic defence review, fusion doctrine.

In 2015 through the UK *National Security Strategy and Strategic Defence Review*, the Government recognised the growing threat to our national stability, security and prosperity from activities occurring in, and from, cyberspace. Our national cyber capability supports our strategic objectives through three core functions: preventing conflict and threats materialising; protecting the UK and its overseas territories from attack particularly (but not exclusively) in, and through, cyberspace; and projecting influence and power rapidly and responsively, either directly from the UK or as part of an expeditionary operation.¹ These are national functions and the military has a contributory role in each, yet we recognise that any military contribution sub- and post-threshold, must be viewed as an extension of politics.² Thus, the military contribution is very much a supporting func-

¹ Ministry of Defence, "Cyber Primer," Second Edition (Shrivenham, UK: Development, Concepts and Doctrine Centre, July 2016), 2.

² Pre- or sub-threshold may be considered as an ability to deliver mass (and un-attributable) effect without triggering a meaningful response, thus blurring what has been

tion of a wider fused, pan-national response and applied in accordance with applicable law, including—where a state of armed conflict exists—International Humanitarian Law (aka Law of Armed Conflict or the Law of War). In this short article, we seek to outline the military contribution to a national approach and how existing international legal and normative frameworks provide a sufficient basis for operations in, from and through cyberspace.

While cyberspace is recognised as a warfighting domain in NATO and UK national military doctrine, it also has far-reaching non-military aspects that affect our daily life.³ For these reasons, activities in cyberspace must be compliant with the rules-based international system. As such, we recognise that there are boundaries of acceptable state behaviour in cyberspace, just as there are everywhere else. In 2013, the UN Group of Governmental Experts on the use of cyber technologies affirmed the application of existing international law to states' cyber activities. On 26 June 2015, the UN Expert Group, including not just the UK and the US but also Russia and China recognised that the UN Charter applies in its entirety to cyberspace. The Group affirmed the relevance of a state's inherent right to act in self-defence in response to a cyber operation meeting the threshold of an armed attack. In addition, the 2015 Report confirmed that the fundamental protections of international humanitarian law—necessity, proportionality, humanity, and distinction—apply in cyberspace.

A version of this article has been presented to a recent Cyber Norms conference held at MIT, Boston. Much of what we say has resonance with this publication and we have therefore used our previous work as a foundation for inclusion in this journal.

Accordingly, Defence's cyberspace activities, whether enabling military action or supporting wider government activities, extend across the continuum of inter-state activity from peace, through cooperation, competition, confrontation, conflict, and War. The reality of increased hostile state activity through cyberspace and below the threshold of armed conflict infers increasing concern of the growing risk of increasingly destructive cyberattacks, as well as potentially the non-intended collateral damage effects of an attack elsewhere on our own infrastructure. This reality requires us to look at how the military instrument might be employed to counter such threats and activities in a period of persistent competition and below the threshold of armed conflict.⁴ To address this requirement, we should unpack some of the themes that might be derived from the title, such as 'response', 'fusion', 'discretion': the 'should' or 'could' and place them into the wider context including framing a five domain—that is an inte-

normal, and hence tolerable, state competition. This is not simply a narrow band which sits on the boundary of peace and war but a fluid and variable space which can be manipulated across time, domains and environments.

³ Joint Doctrine Publication 0-01 UK Defence Doctrine, 6th Edition (Draft).

⁴ "Persistent competition" might be defined as intense hostile state activity outside the rules-based international system and below the threshold that might result in armed conflict.

grated air, space, cyber, maritime, and land—military contribution through our Joint Action operating model to achieve the military objective of a national strategy.⁵

First, the use of the word ‘response’ has significant negative connotations – it is reactive and implies a degree of passivity before action. All too frequently, we see response used in conjunction with military – “the military response.” But this hides the inherently offensive nature, and the utility of pre-emptive qualities, of the military instrument. It must be recognised that hard kinetic action is not always appropriate or indeed necessary. The military has more to offer than just binary offensive or defensive capabilities. So, the point to emphasise here is that there is a broad range of military options that have wide utility for application, contributing to a fused national approach left of an adversary’s strike or in the zone of sub-threshold persistent competition. This could be to either contribute to an anticipatory deterrence or coercion strategy as well as to contribute to our overall national security approach. Yet, we should recognise that the military contribution may not, of course, be a cyber one. So, our ability to contribute more effectively “left of bang” as we like to say, requires resource and political appetite to do so. It must be exercised and tested to prove the approach – and this should not be solely a military enterprise. It needs to be ‘fused’ with others – the Intelligence agencies, government, other government departments, industry, and the critical national infrastructure as examples. We talk of persistent competition from our adversaries; therefore, our approach must be one of persistent engagement—physical, virtual and cognitive—utilising all levers of national power, diplomatic, information, economic, and military to demonstrate national resolve and determination but also to ensure we retain a competitive advantage.

This leads on to ‘fusion’ and, by implication, the UK Government’s Fusion Doctrine. The principles behind Fusion Doctrine, we contend, are nothing new. We have had an “integrated approach,” “comprehensive approach,” and the “full-spectrum approach” – all designed to fuse cross Whitehall activity. Yet, the Fusion Doctrine goes further as it inculcates a real sense of joined-up thinking and practice to deliver successful outcomes against multiple challenges. A strategy to deter adversaries is a key function of the Fusion Doctrine. And the deterrence of cyber aggression or cyberattacks needs to include all aspects of our national life with all sectors ensuring that they should consider their response, not in isolation, but coherent, consistent, and coordinated with others. As a result, our approach to modern deterrence is somewhat different from the deterrence

⁵ “Joint action” is our framework approach to integrate information activities with fires (lethal and non-lethal effects), manoeuvre and outreach to gain competitive advantage – placing influence as a primary outcome, and integration at its core as the principal enabling tenet. Tempo and the precision of effect will continue to be generated, predominantly (but not solely), by a joint force, planning and executing operations within and across multiple domains rapidly, to maintain the initiative and pose the adversary with multiple insoluble dilemmas.

of the Cold War. Deterrence today needs to be a more nuanced use of hard and soft power with all departments contributing to fused strategies to deliver specific deterrence strategies for specific threats and behaviours.

So, what 'could' the military do? This needs to be broken down into two parts: the generic contribution, what we do, and care for, in support of Government priorities as well as the specific cyber role. Turning first to our generic contribution.

Through the military, the Government exercises its right to the legitimate use of force and such force is used to further political objectives, primarily the security of our nation. Our objectives are clearly defined in the National Security Strategy and within defence policies. From these objectives, a range of military tasks is defined and resourced.

Possession of capable, professional, and well-trained militaries also gives governments a broader set of response options to cyber threats. As the former UK Attorney General said, "States that are targeted by hostile cyber operations have the right to respond to those operations in accordance with the options lawfully available to them..."⁶ A hostile cyber operation does not necessitate a cyber response. All lawful options, including an armed response when appropriate, are open to states that are attacked.

While the UK's armed forces are primarily resourced and configured to defend our national security, our broad maritime, land, air, space and cyber capabilities can be made available to support other crises, such as humanitarian aid and military aid to government departments. Thus, our response to a crisis or event brought on by actions in cyberspace could include the full range of conventional military capabilities to the use of limited or discrete functions and roles. This is not dissimilar to that seen during the foot and mouth outbreak in the UK in 2001, the fire service strikes or during flooding where military capability has been used to reinforce governmental departments or civilian organisations. But one area where the military could provide a very worthwhile generic support function is through our command and control organisations which are designed around the delivery of an integrated, cross-function liaison, coordination, and control output. These headquarters are adept at fusing multi-source intelligence and information to direct activities and would also be able to communicate the defence contribution and ensure that it is dovetailed into wider narratives. Our headquarters are also good at applying the rules of engagement and standards of proportionality and discrimination on the use of military capability – whether it be a non-lethal or lethal force. Thus, we believe that the military is good at self-restraint and uses tested processes to increase and decrease the use or the threat of force to achieve the desired outcome. We also utilise "plugs and sockets" to introduce non-organic or non-defence structures into our decision-making architecture. Combined, this allows effective, rapid, and evidence-based decision-making processes.

⁶ Speech by Jeremy Wright QC to Chatham House on 23 May 2018.

Let us turn to the specific cyber contribution. Our UK doctrine clearly spells out how defence breaks down its operations in cyberspace and how these contribute to delivering military effect and supporting wider political objectives. We will not go into the detail here—much of it remains classified—but it is safe to say that our doctrine outlines the following cyberspace functions: defensive⁷ (active⁸ and passive⁹) as well as offensive¹⁰ cyber operations, cyber intelligence, surveillance and reconnaissance¹¹ and cyber operational preparation of the environment.¹²

From the perspective of what the military ‘*should*’ contribute, our approach is twofold. First, we must continue to mainstream our cyberspace thinking and actions across our whole force. Doctrine and education are key here. Because of the sensitive nature of the cyber domain, our doctrine is currently classified, and this has limited its accessibility and hampered our ability to increase understanding of cyber operations across the UK military. We are now exploring ways to increase the accessibility of our cyber doctrine to enhance its application as part of our approach to developing five domain integration (maritime, land, air, space as well as cyber). In parallel, we are embarking on a journey to develop some cutting-edge conceptual thinking to guide future iterations of our doctrine, education, and practice. Combined, these will increase our cyberspace awareness, our agility, and, therefore, our utility by generating warfighters capable of operating in cyberspace rather than producing cyberwarriors – although we do need some of the latter! The second element must continue to bring focus on what we need to do to ensure our networks and interfaces are as resilient as possible and that our defensive measures are consistent and coordinated with those who legitimately have access to or share our systems. This is not an easy challenge, especially the need to ensure cyber resilience in all our developmental programmes as well as ensuring that our legacy programmes and capabilities can adapt to the rapidly changing threat dynamics in cyberspace now and into the future.

So, to conclude, the military can provide a significant contribution to the cyber threat and much of that is already in train. We must also recognise that undoubtedly the largest contributions we can make are threefold. First, ensuring our own cyber defence is robust and resilient, including guaranteeing that it is consistent and coordinated with the defensive approaches of others who share our networks. Second, our response or contribution may not be in the cyber do-

⁷ Active and passive measures to preserve the ability to use cyberspace.

⁸ Activities that target hostile offensive cyber operations to preserve our freedom of manoeuvre within cyberspace.

⁹ Threat specific defensive measures to reduce the effectiveness of cyber activity.

¹⁰ Activities that project power to achieve military objectives in, or through, cyberspace.

¹¹ Intelligence, Surveillance and Reconnaissance (ISR) activities in, and through, friendly, neutral and adversary cyberspace to build understanding.

¹² All activities conducted to prepare and enable cyber ISR as well as defensive and offensive operations.

main itself. Third, our command and control structures provide a very useful reference point from which we could develop a fused strategic headquarters that coordinates and directs our national cyberspace operations. These can only be realised if Defence continues to invest in mainstreaming cyberspace as both a threat and opportunity in our strategies, doctrine, and practice. Yet returning to the question, effective fusion can only be achieved through practice, exercising, and testing ... until it becomes second nature.

Disclaimer

The views and opinions expressed are solely those of the contributing authors and should not be taken to represent those of Her Majesty's Government, Ministry of Defence, Her Majesty's Armed Forces or any UK government agency, the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.



Israel Defense Forces and National Cyber Defense

Lior Tabansky

Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv University

Abstract: Cybersecurity in and of itself is not particularly new. Contemporary opportunities to exploit vulnerabilities, however, make this a challenging field. It is only natural that rivals exploit newly created opportunities. Conflict, in which adversarial relationships have a cyber dimension, is here to stay. Accordingly, societies must devise an appropriate organization to protect themselves from intentional threats. This article surveys Israel's approach, outlining the origins and the evolution of the national cyber defense, prevailing threats, doctrinal challenges, and the role military services play in cyber defense.

Keywords: Cybersecurity, cyber defence, strategy, doctrine, cyber operations, roles of the Israel Defense Forces.

Michael Warner, the Cyber Command Historian at the U.S. Department of Defense, outlined the main theoretical insights for American policy-makers and officials: Computers can spill sensitive data and must be guarded (1960s); Computers can be attacked and data stolen (1970s); We can build computer attacks into military arsenals (1980s and 1990s); Others might do that to us – and perhaps already are (1990s).¹ But new opportunities to exploit vulnerabilities make this a challenging field. It is only natural that rivals exploit such newly created opportunities. Cybered conflict, meaning that all adversarial relationships have cyber dimensions, is here to stay.² Accordingly, societies must devise and establish ap-

¹ Michael Warner, "Cybersecurity: A Pre-History," *Intelligence and National Security* 27, no. 5 (2012): 781-799, <https://doi.org/10.1080/02684527.2012.7085>.

² Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens, GA/London: The University of Georgia Press, 2011).

propriate organizations to protect themselves from (intentional) threats. This article surveys Israel's national cyber defense origins, threats, and challenges.

Israel's National Security Strategy and Current Strategic Environment

The core of Israel's security doctrine has always included:

- Absolute numerical inferiority³
- An acute lack of strategic depth⁴
- Constant regional volatility
- Protracted or irresolvable Arab-Israeli conflict
- Self-reliance in defense.

From the 1990s to 2010s, Israel's strategic landscape has shifted from threats originating in the Arab militaries to threats originating in irregular or semi-regular sub-state organizations supported by Iran. Iran, which is neither Arab nor a neighbor of Israel, poses a potential nuclear challenge of the highest magnitude and requires separate treatment. In contrast to states, organizations such as Hezbollah, Islamic Jihad, or Hamas build on a radical Islamist ideology denying Israel's right to exist. Their doctrine of resistance—*Muqawama*—assures its adherents that the long, historical, currently difficult struggle against Israel will eventually end in victory, despite temporary setbacks.⁵ Hezbollah, Islamic Jihad, or Hamas organizations promise and claim success to their audiences, whereas Arab have states failed to defeat Israel. Yet Israel withdrew unilaterally from southern Lebanon in May 2000, disengaged from the main Palestinian popula-

³ The combined population of the Arab states amounts to hundreds of millions, while Israel remains several orders of magnitude smaller. As of 2017, Israel was home to slightly more than 6.5 million Jews compared to some 400 million residents of the member countries of the Arab League – more than a third of them in countries bordering Israel.

⁴ Yaakov Amidror, "The Evolution and Development of the IDF," in *Routledge Handbook on Israeli Security*, ed. Stuart A. Cohen and Aharon Klieman (Routledge, 2018), states: "From its very inception the State of Israel (and before it, the pre-state Jewish Yishuv) had to confront an existential security threat – a narrow territorial entity with its back to the Mediterranean Sea, surrounded on all sides by Arab foes sworn to its extinction. The distance from the Mediterranean Sea eastward to the mountainous area overlooking and dominating the coast—known as the "West Bank" and overwhelmingly populated by Palestinian Arabs—is merely 12 km at its narrowest (from Netanya to Tulkarm); and from Tel Aviv a mere 25 km (16 miles) at its widest. Even when adding the West Bank to the equation, the country's total width is less than 60 km. Israel's economic, financial, technological and demographic center is heavily concentrated along the Mediterranean seacoast on a narrow strip of just 100 km between Haifa and Ashdod."

⁵ Efraim Inbar and Eitan Shamir, "'Mowing the Grass': Israel's Strategy for Protracted Intractable Conflict," *Journal of Strategic Studies* 37, no. 1 (2014), <https://doi.org/10.1080/01402390.2013.830972>.

tion centers in the West Bank after the Oslo accords and again in 2002, and evacuated its civil and military presence from the Gaza Strip in August 2005.

Israel's de-facto security strategy now includes four pillars:

- I. Early warning
- II. Decisive battlefield victory
- III. Deterrence (cumulative, not absolute)
- IV. Defense of the rear "home front."

The fourth—defense—has been added gradually after the lessons of the 1991 Iraq's ballistic missiles strikes, Palestinian terrorism, and the massive rocket threat from Lebanon and the Gaza strip. Supported by Iran, *Hezbollah* and *Hamas* deploy a massive firepower of more than 120,000 missiles and rockets aimed at Israel's cities. Iran drives modernization of their mostly short-range, low-precision arsenal to include precision-guided medium-range rockets. Israel's current operational arena has erased any meaningful distinction between military fronts and the civilian rear. The IDF increasingly invests in state-of-the-art military technologies to find ways to defend the "home front." The IDF cannot consider failure even at the tactical level, let alone think in terms of a protracted stalemate in future wars. Should deterrence or combat fail, neither Israelis nor the IDF will be given a second chance.

Unlike most Western militaries, cyber threats are not top of Israel's security agenda simply due to the high intensity of non-cyber threats ranging from terrorism to massive trajectory projectiles to missiles and Iran's nuclear program. Nevertheless, Israel has been one of the most advanced nations when it comes to the role of government in national cybersecurity. Non-military organizations performed the vast majority of cybersecurity.

The following sections present the civilian element first, and then the roles of the IDF.

The Evolution of Israel's National Cyber Strategy

Critical Infrastructure Protection Arrangement of 2002

Despite the prevalence of much more lethal and urgent non-cyber national security threats, Israel's government has been delivering Critical Infrastructure Protection (CIP) since 2003.

With a thorough understanding of civilian infrastructure and cyber vulnerabilities garnered from years of defense experience, at the turn of the century MAFAT (the Ministry of Defense R&D Directorate) communicated its concerns regarding the vulnerabilities of critical civilian infrastructure to other government branches. Eventually, the government then tasked the National Security Council (NSC) with outlining strategies to cope with the emerging risks. This resulted in the December 11, 2002 Government of Israel Special Resolution B/84 on "The responsibility for protecting computerized systems in the State of Israel." Israel created a CIP regulation that required supervised organizations to

appoint and employ dedicated IT-security personnel responsible for implementing the professional instructions of a government agency. The state decided to form a new CIP organization: *Re'em* (the National Information Security Agency, NISA). *Re'em* enjoyed the appropriate legal foundation in the 'Regulation of Security in Public Bodies Law of 1998' and the *Shabak* (Internal Security Agency) Statute. The supervised, privately-owned businesses and state-owned utilities maintain financial responsibility for all operations, protection, maintenance, upgrading, backup, and recovery of its critical IT systems—including the changes, enhancements, and equipment mandated by *Re'em*—all while sharing information and activities with the regulator. Finally, the law specified sanctions against executives of supervised organizations neglecting the mandatory requirements set by *Re'em*.

This Critical Infrastructure Protection arrangement has been in place since the B/84 Resolution of 2002. Since then, the government and defense sectors have fended for themselves, as Israel Police dealt only with strictly criminally defined cases of cybercrime. Therefore, as the first decade of the 21st century came to a close, this left the lion's share of the population—small-medium business (SMB), Non-Government Organizations (NGOs), and general citizenry—without cybersecurity. As the technology evolved, threat scenarios grew but received no treatment. These include potential disruption of civil services, accumulation of small-scale incidents in SMBs, risks to 'concealed' or embedded computers (such as navigational devices or controllers in cars), and degrading societal morale and resilience by cyber means (e.g., Influence operations via Social Media). Yet, only the experts dealt with the topic.

The National Cyber Initiative Expert Review

The public discovery of Stuxnet in 2010 propelled cybersecurity to the top of policy agendas worldwide. Prime Minister Benjamin Netanyahu approached Major-General (Res.) Professor Isaac Ben-Israel, who at that time was the Chairperson of the National Council for Research and Development in the Ministry of Science, to review cybersecurity and recommend a policy for Israel. Professor Ben-Israel accepted the task, and the National Cyber Initiative was launched in 2010 with the vision:

to preserve Israel's standing in the world as a center for information-technology development, to provide it with superpower capabilities in cyberspace, to ensure its financial and national resilience as a democratic, knowledge-based and open society.

The National Cyber Initiative addressed three main issues:

- How to incentivize and develop cyber technology in Israel to ensure its position as a (top five) world leader by 2015?
- Which infrastructures are required to develop cyber technology in Israel?

- What arrangements are required to best deal with the risks and threats in cyberspace?

The National Cyber Initiative thus clearly dealt with more than a narrow-defined national security. The composition of the task force reflected the initiative's broad vision and integrated approach. Consequently, for six months, 80 experts—defense and military representatives, academic experts, research and development institutional directors, and representatives from the relevant ministries—performed a systematic overview of the challenges and opportunities. The team was divided into eight subcommittees, one of which was classified.

Israel's National Cybersecurity Strategy of 2011

The Government Resolution No. 3611 of August 7, 2011 “Advancing National Cyberspace Capabilities”⁶ accepted the National Cyber Initiative's recommendations and it is Israel's public National Cybersecurity Strategy. Like all official high-level National Cybersecurity Strategy documents, it is a “grand strategy” that declares the vision and the guiding principles. Subsequent strategies in each domain have been derived from this grand strategy.

The main recommendation was to establish a dedicated government agency to lead cyber efforts across public and private Israeli stakeholders and to coordinate policy instruments. Further, the document recommended:

1. to establish a National Cyber Bureau (hereafter: The Bureau) in the Prime Minister's Office;
2. to regulate responsibility for dealing with the cyber field;
3. to advance defensive cyber capabilities in Israel and promote research and development in cyberspace and supercomputing;
4. to provide a budget for the implementation of the Resolution, proposed by the Prime Minister in consultation with the Minister of Finance and submitted to the government for approval within two months of passing this Resolution.

The Israel National Cyber Bureau (INCB)

To develop and implement the grand-strategy, the Israel National Cyber Bureau (INCB) was established in the Prime Minister's Office (PMO).⁷ Res. 3611 defined its mission and roles as follows.

⁶ Government decision 3611: Promoting national capacity in cyber space (Jerusalem, Israel, PMO Secretariat).

⁷ Dr. Eviatar Matania was named head of the INCB. He established the organization and directed its work. He served two three-year terms, remaining in duty until the end of 2018.

*Mission:*⁸ The Bureau functions as an advising body for the Prime Minister, the government and its committees, which recommends national policy in the cyber field and promotes its implementation, in accordance with all law and Government Resolutions.

Roles:

- To advise the Prime Minister, the government and its committees regarding cyberspace. In matters of foreign affairs and security, the advice provided to the government, to its committees and to the ministers, will be provided on behalf of the Bureau by means of the National Security Council.
- To consolidate the government's administrative work and that of its committees related to cyberspace; to prepare them for their discussions and follow-on implementation of their decisions. In matters of foreign affairs and security, the consolidation of administrative work, preparation for discussions and follow-up on implementation of decisions will be carried out by on behalf of the Bureau by means of the National Security Council.
- To make recommendations to the Prime Minister and government regarding national cyber policy; to guide the relevant bodies regarding the policies decided upon by the government and/or the Prime Minister; to implement the policy and follow-up on the implementation.
- To inform all the relevant bodies, as needed, about the complementary cyberspace-related policy guidelines resulting from Government Resolutions and committee decisions.
- To determine and reaffirm, once a year, the national threat of reference in defending cyberspace.
- To promote research and development in cyberspace and supercomputing in the professional bodies.
- To work to facilitate the cyber industry in Israel.
- To formulate a national concept for dealing with emergency situations in cyberspace.
- To conduct national and international exercises to improve the State of Israel's preparedness in cyberspace.
- To assemble intelligence from all parties in the intelligence community regarding cyber security.

⁸ The mission, roles, and tasks of the Israel National Cyber Bureau (INCB), presented in this section, are defined in "Advancing National Cyberspace Capabilities," Resolution No. 3611 of the Government, August 7, 2011, available at https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Israel_2011_Advancing_National_Cyberspace_Capabilities.pdf.

- To assemble the national situation status regarding cyber security from all relevant parties.
- To advance and increase public awareness to threats in cyberspace and the means of coping with them.
- To formulate and publish warnings and information for the public regarding cyber threats, as well as practices for preventative behavior.
- To advance the formulation of national education plans and the wise use of cyberspace.
- To advance cooperation in the cyber field with parallel bodies abroad.
- To advance coordination and cooperation between governmental bodies, defense community, academia, industrial bodies, businesses and other bodies relevant to the cyber field.
- To advance legislation and regulation in the cyber field.
- To serve as a regulating body in fields related to cybersecurity, as detailed in Article I of Addendum B.
- To carry out any other role in the cyber field determined by the Prime Minister, in accordance with all laws and Government Resolutions.

Tasks:

The Head of the Bureau was tasked to submit to the Prime Minister, within 90 days of his appointment, a detailed work plan based on the working principles outlined by the Chairman of the National Council for Research and Development (NCRD), Prof. Maj.-Gen. (Ret.) Isaac Ben Israel, including:

- to approach the Council for Higher Education (CHE) and the Planning & Budgeting Committee (PBC) and request that they examine the possibility of establishing an academic cyberspace research center;
- to promote the establishment of a national center of knowledge for high-performance computing. If the center is academic, the *Malag* and *Vatat*⁹ should be approached and asked to examine the matter;
- to establish infrastructure to develop cyber technology, such as developing simulation capabilities and national accreditation of cyber technology;
- to improve export procedures relevant to cyberspace and proper oversight of exports in this field;
- to develop tools for coping with cyberspace emergencies;
- to develop a national cyber defense;
- to develop solutions for defined cyber defense challenges;
- to develop domestic cyber solutions and technologies.

⁹ See dedicated sections below.

Balancing Basic Liberties and Security Needs

In June 2013, Edward Snowden began leaking secret documents he had stolen, revealing numerous global surveillance programs, many run by the United States' NSA, Australia's ASD, the United Kingdom's GCHQ, and Canada's CSEC often with the cooperation of telecommunication companies. These intelligence agencies collected bulk information and Snowden, among others, argued that these programs were degrading citizen's rights, especially to privacy, and were also violating domestic laws. Apparently, NSA taps directly into the servers of major internet firms, including Facebook, Google, Microsoft, and Yahoo, to track online communication using a surveillance program known as Prism.

At the time, the young INCB was focusing on force buildup, while the mature *Re'em* focused on CIP operations. As *Re'em* had been a unit of the *Shabak*, a potential risk loomed in the background. *Shabak* has a clear primary mission. A security or counter-intelligence organization that has access to other people's networks for a separate mission might take advantage of this access to a certain extent. It is true that *Shabak* had never abused the CIP assets for their purposes. It is also true that *Re'em* has had a good track record of success and that civilian oversight over *Shabak* had been well developed by 2010s. Nevertheless, the Snowden-NSA revelations propelled the liberties-security tensions to the top of the public debate as well as policy agendas. Any subsequent milestones in Israel's strategy must be set against this backdrop.

The National Cyber Security Authority (NCSA)

The Israeli government Resolution 2444 of February 15, 2015 established the National Cyber Security Authority (NCSA) to protect Israeli civilian cyberspace.¹⁰ The NCSA was set up alongside the INCB in the PMO. Unlike CIP or cybersecurity agencies elsewhere, the NCSA has not been given any law-enforcement activities. This is a deliberate attempt to prevent any ongoing suspicion of NSA-like practices, to build trust, and to facilitate cooperation with all relevant cybersecurity stakeholders in the society. This unique design is intended to reduce the tension between basic freedoms and security, and to increase societal trust in this government authority. Following the same logic, the resolution is that NCSA incorporates the CIP organization *Re'em*. Indeed, it was transferred from the ISA (*Shabak*) to the NCSA in a process that took about a year.

The Authority began operations in the PMO on April 1, 2016, 90 days after Mr. Buki Carmeli was appointed head of the Authority. During the annual Cyber-Week held by the Blavatnik Interdisciplinary Cyber Research Center (ICRC) of Tel Aviv University in June 2017, the NCSA held a one-day unveiling event, introducing its leadership and plans to a 600-strong audience. All the leaders of the NCSA presented their views and ideas. The head of the NCSA, Buki Carmeli, used the following water supply analogy to describe his vision of the NCSA:

¹⁰ This decision was made after several rounds of extensive consultations, accepting Prof. Ben Israel's official recommendations.

We (NCSA) approach civilian cybersecurity as public water system. We are concerned with uninterrupted supply of clean water throughout the society. When we will find contamination, we will not suspect who contaminated it, by negligence or malicious intent.

In 2017, all the cyber Bureau's technological activities were integrated into the Cyber Technologies Unit, which is the national technology arm for advancing cyber capabilities and technologies on a national level.

The Computer Emergency Response Team – Israel (CERT-IL)

Centered on cooperation, the NCSA has been developing a concept and the technology to enhance national situational awareness and security in cyberspace. The NCSA has established and operates the new National Computer Emergency Response Team (CERT-IL) to become a central public contact point for support for all civilian non-critical sectors. It is the central pillar in the long-term effort to secure Israel's civilian sector at large. While developing channels to work with sensitive data and clandestine agencies, CERT-IL must remain accessible to any civilian.

CERT-IL was planned and built in the Be'er-Sheba CyberSpark complex and began operations on July 1, 2014. An industrial consortium led by the Israeli defense contractor RAFAEL won the tender and built the CERT-IL.

The Israel National Cyber Directorate (INCD)

In accordance with Resolution 2444 of 2015, the NCSA, the operative body for cyber protection, and the INCB, responsible for the policies and the cyber force buildup, jointly constituted the National Cyber Directorate operating from the Prime Minister's Office, directly under the Prime Minister. The head of the Cyber Bureau was also appointed head of the Directorate and was put in charge of approving the work plans of the Authority and the budget of the Bureau. With the establishment of the NCSA, the guiding principle to insulate force buildup from daily needs led to a separate organization. Within two years, despite a good track record, the disposition changed towards a unified structure with a simpler hierarchy. To streamline the work, the Government of Israel Resolution 3270 of December 17, 2017 merged the Bureau and the Authority into the National Cyber Directorate, to be responsible for all aspects of cyber defense in the civilian sphere, from formulating policy and building technological power to operational cyber defense.¹¹

¹¹ During this time, as Dr. Matanya completed his six-year term as Head of the Directorate, Mr. Yigal Unna was named his successor and took office at the beginning of 2018. Dr. Matanya then joined Tel Aviv University as Professor and Head of the Security Studies Program. See https://www.gov.il/he/Departments/policies/dec_3270_2017.

Strong Engagement of The Private Sector, NGOs and Academia

The strategy is entirely cooperative, and in fact, the INCD has initiated, financed, and coordinated multiple efforts throughout Israel's economy. One example is the establishment and co-financing of Cyber Research Centers in most of the research universities in Israel. These academic centers of excellence perform independent scientific research. Another example is the establishment and co-financing of several innovation incentive programs in partnership with the Israel Innovation Authority. As for cybersecurity promotion throughout society, the INCD does not intend to introduce any additional regulations and, instead, has opted for cooperative work with existing regulators.

IDF: Roles and Responsibilities in National Cyber Defense

The MoD and the IDF do not assume that their mission is to defend the entire society. The defense sector defends itself in cyber, whilst the INCD caters for all the rest. Such a division is common to all Western democracies.

As cybersecurity has become a profound risk, what does the IDF do about it? Major-General (Res.) Amidror writes:

The IDF, like other militaries, is pre-occupied with working out how best to integrate cyber capabilities, for both defensive and offensive purposes. Since it is clear that cyber warfare will become hugely important in the coming years, and because there is a long road ahead, the IDF is already investing considerable sums of money and highly talented personnel in this area and is engaged in the deep and broad development of its cyber capabilities. How to organize the new units responsible for cyber, the relationship between offensive and defensive efforts, and the ratio between them – remain huge challenges.¹²

Current public sources suggest the following organization of Computer network operations (CNO) in the IDF.

Alleged Operations

On September 6, 2007, the IAF successfully bombed and destroyed a building complex in Al-Kibar, near the city of Deir ez-Zor in eastern Syria. The building hid the construction of a graphite-cooled nuclear reactor: almost an exact copy of the plutonium reactor in North Korea.¹³ The attack on the Syrian reactor project echoes the daring 1981 IAF raid, which destroyed the *Osirak* nuclear reactor in Iraq. But this time, a cyberattack was, allegedly, central to operational success: overcoming the dense Syrian air defense. According to foreign sources, the extensive Syrian air defense systems failed to identify the eight IAF fighter aircraft in the monitored airspace. These sources assume that Israel infiltrated and tem-

¹² Amidror, "The Evolution and Development of the IDF."

¹³ Elliott Abrams, *Tested by Zion: The Bush Administration and the Israeli-Palestinian Conflict* (Cambridge University Press, 2013).

porary neutralized the Syrian air defense radars and communication systems in a cyber-attack. This 12-year old operation demonstrates the blurred line between electronic warfare and the cyber-warfare capabilities. Either way, it appears that a cyber-attack can play a supporting role for a kinetic strike.

The public disclosure of the Stuxnet malware in July 2010 and its subsequent analyses were an eye-opener for the public. Crucially, Stuxnet proved that a cyber-attack could indeed cause significant physical destruction. As Demchak and Dombrowski write:

The Stuxnet method and its success thus changed the notion of vulnerability across increasingly connected societies and critical infrastructures. The days of cyber spying through software backdoors or betrayals by trusted insiders, vandalism, or even theft had suddenly evolved into the demonstrated ability to deliver a potentially killing blow without being anywhere near the target.¹⁴

The malware slowly damaged the centrifuges at the Natanz nuclear enrichment facilities in Iran by reprogramming the Siemens programmable logic controller (PLC) that ran the centrifuges and caused it to spin the motors out of the safe range. The stealthy, persistent attack within a secured air-gapped network had to first compromise a Microsoft Windows system and then propagate inside corporate networks to reach the programmable logic controller (PLC). By the end of 2010, Stuxnet had infected approximately 100,000 hosts in dozens of countries, 60 percent of which were in Iran.¹⁵ Uniquely, Stuxnet infection does not equal damage. Stuxnet executed its weaponized payload (the PLC code supposedly altering the centrifuge rotation speed) only where the specific hardware and software configuration was found. No damage was done to an infected system that did not meet the precise set of predefined attributes.¹⁶ Stuxnet is thus a precision-guided weapon: a cyber-attack that causes physical destruction but only to a specific target.

C4I & Cyber Defense (AGAF HA-TIKSHUV VEHAHAGANA BISVIVAT RESHET)

In June 2015, the IDF published the decision to unify cyber units of the General Staff's C4I (command, control, computers, communications, and intelligence) branch and Military Intelligence under a single command by 2017. The IDF then reversed this plan to integrate defensive and offensive capabilities.

In May 2017, the IDF General Staff renamed the C4I branch (that was established in 2003) to The C4I & Cyber Defense branch. A recently established IDF Cyber Defense Division was merged into the C4I branch. C4I is now responsible

¹⁴ Chris C. Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 32-61.

¹⁵ Kim Zetter, *Countdown to Zero Day : Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014).

¹⁶ Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 365-404, <https://doi.org/10.1080/09636412.2013.816122>.

for network security within the IDF and remains responsible for IDF's Computer Network Defense (CND) and relevant Computer Network Exploitation (CNE). Moreover, the C4I will remain a central player in Israel's cybersecurity as it includes:

- training of IDF's Information and Communication technology professions;
- software development for the IDF;
- ICT system architecture for the IDF;
- cryptographic foundations development for the IDF and Israel at large.

The C4I & Cyber Defense branch aims to advance the vision of a single IDF network. However, insufficient cooperation, friction, and conflicts of interest between air and ground forces remain an unsolved problem in the IDF. Nevertheless, while ICTs have contributed to closer consultation, communication, and coordination during the last few years, this does not automatically create jointness.

This is not to accuse the IDF of a lack of jointness. In the business sector, one finds no less glaring siloes and uncoordinated activities as in any advanced military. With the increasing adoption of tailored cyber technologies within military siloes, the digital gaps between "elite" and common units are mounting. If left unattended, these developments may further impede jointness as well as prevent the coordination of cyber warfare throughout the IDF and other defense organizations in Israel.

This vision, of course, faces significant challenges: many of IDF's units and branches have developed and are operating diverse Information and Communication Technologies solutions on dissimilar infrastructures. A more likely outcome for the vision would be the unification of digital infrastructure within the IDF Ground Forces: C4I's natural domain.

Military Intelligence (Agaf haModi'in – Aman)

Intelligence organizations have been the pioneers of cyber technology, amassing operational experience while remaining a step ahead of civilian capabilities. Israel's strategy puts a premium on both early warning and qualitative edge. These two factors are among the reasons why Israel's intelligence organizations have earned a formidable cyber reputation.

Aman is an independent service that is not part of the ground forces, the Navy, or the Air Force. *Aman* Unit 8200 is responsible for collecting signal intelligence (SIGINT) and for code decryption. According to intelligence analysts, 8200 is similar to the NSA or Britain's Government Communications Headquarters (GCHQ), often covering the entire intelligence cycle. Foreign sources assert that Unit 8200 contributed to Stuxnet, Flame, Duqu, and other sophisticated cyber campaigns for offense and intelligence.

Even so, Military Intelligence remains responsible for both Computer Network Attack (CNA) and relevant Computer Network Exploitation (CNE).

The Israeli Air Force (IAF)

The Israeli Air forces view combat as the application of advanced high technology in waging war. The airplane embodies the supremacy of the advanced technology.¹⁷ The IAF service culture is based on central command and control and supporting communications¹⁸ and it aims to have a complete picture of the entire airspace in real-time. Headquarters accurately plan each air mission; time schedules are precise, determined by distance, flight path, evasion maneuvers, payload weight, and the amount of fuel. The IAF has developed and controlled its own supporting functions: Logistics; Command, Control, Communications, Computer (C4); Intelligence; Electronic Warfare (EW) and Special Force (the *Shaldag* unit) – all critical for air dominance. Practically, everything in the IAF depends heavily on advanced digital Information and Communication Technology. The IAF operates its own intelligence (*Lahak Modi'in – Lamdan*). As the IAF entirely depends on digital ICTs, the need to secure them was a consideration in design and operation, contributing to enhanced cyber maturity in the IAF. Moreover, the IAF has a separate and more advanced infrastructure than the other IDF branches.

Spillover Effects of Defense R&D

In the mid-90s, Israel was a welfare state with a struggling economy and a negligible hi-tech industry. Just a few years later, while still coping with demanding security issues, Israel has developed into a technological giant with a sophisticated and innovative hi-tech sector. Today, the representation of Israeli hi-tech companies in the National Association of Securities Dealers Automatic Quotation System (NASDAQ) outstrips economic and technological superpowers such as Britain, Germany, Japan, and South Korea, and, for over a decade now, Israel has been one of the leading innovation hotbeds in the world. The IDF has created two spillover effects, which have contributed to Israel's success in high-tech and cybersecurity.

Given its overwhelming geographical and numerical inferiority, Israel's security strategy has been emphasizing a qualitative advantage that includes human skills, moral and scientific-technological superiority. The IDF perceives cyber technology as an important, broad, qualitative force multiplier. As in the US, several IDF branches and non-military intelligence organizations have long paid close attention to the development and exploitation of electronic warfare, signal intelligence, encryption and information security, computer warfare and information warfare. Almost three decades ago, several stakeholders within the IDF had already invested significant efforts in radical innovations that today would be termed "cyber warfare." Like DARPA in the US, *Maf'at* (the Ministry of De-

¹⁷ Allen W. Batteau, "The Anthropology of Aviation and Flight Safety," *Human Organization* 60, no. 3 (Fall 2001), pp. 201-211.

¹⁸ Amidror, "The Evolution and Development of the IDF."

fense Directorate for Defense Research & Development, DDR&D) has been driving and facilitating daring innovations in cyber R&D.

Regardless of what the IDF arms request, *Maf'at* can initiate major defense R&D independently. In parallel, the IDF's main cyber stakeholders—Intelligence, C4I, Air and Special Forces—have the capacity to perform tailored R&D and acquisition to support their missions.

In addition to classified R&D, *Maf'at* and the INCB launched a dual-use, civilian and defense cyber R&D plan called *MASAD* in October 2012.

Spillover Effect of Military Human Capital

Swed and Butler postulate that the military socialization process cultivates new skills (human capital), new social networks (social capital), and new social norms and codes of behavior (cultural capital). Those three together are “military capital.” Conscripts absorb the military capital, or part of it, while in service and “export” it into the civilian sphere where it converts well, especially in the hi-tech sector. For instance, improvisation, which is valued as a problem-solving skill in a resource-poor and uncertain environment and is, therefore, encouraged by the IDF culture while not being part of the official IDF code.¹⁹

Israel maintains mandatory conscription of 18-year olds. The IDF regularly trains and develops fresh recruits as well as career officers. Given the three-year mandatory service for males, one can assume that up to one-third of the force will be engaged in various training programs at any given moment. The IDF has long developed an intricate system to assess the conscripts' potential and assign a fitting training and career path to most, significantly contributing to the share of science and technology experts in Israel.²⁰ After the mandatory service, those who received valuable training are more likely to do reserve service than others are.

The profiles of Israeli hi-tech workers contain some very high military capital. Moreover, the job market in hi-tech demonstrates an institutional preference for those with military capital. Indeed, general and military service in technological units is perceived as such an advantage that it often equates to a University degree.²¹

¹⁹ Probably the most organized and influential group is the 8200 association. The name 8200 become hallmark since its graduates were the local hi-tech and venture capital industry vanguards. In comparison to other military veterans, Unit 8200 graduates' military capital convertibility is among the highest. See Ori Swed and John Sibley Butler, “Military Capital in the Israeli Hi-Tech Industry,” *Armed Forces & Society* 41, no. 1 (August 2015), <https://doi.org/10.1177/0095327X13499562>.

²⁰ Gil Baram and Isaac Ben-Israel, “The Academic Reserve: Israel's Fast Track to High-Tech Success,” *Israel Studies Review* 34, no. 2 (2019), <http://dx.doi.org/10.2139/ssrn3269147>.

²¹ Swed and Butler, “Military Capital in the Israeli Hi-Tech Industry.”

Doctrinal Challenges for IDF

Cyber warfare and autonomous systems have clearly become a high defense priority. Which roles will the IDF assign for cyber capabilities? Consider one subset of questions: Should cyber capabilities support kinetic capabilities, should they replace kinetic strikes where possible, or should they deliver effects that will render kinetic force unnecessary? How well will the IDF make use of these? Significant change is as difficult for the IDF as for any other large bureaucratic organization.

Transparency vs. Secrecy

Much of the challenges of cybersecurity are substantial. IDF Military services (in Hebrew 'Zroa') undergo significant rearrangements. However, the IDF cannot shake the habit of obscuring much of its activity, not only from the public but also from competing branches and services. These well-known tendencies to conceal activities impede cooperative intellectual efforts in commercial as well as military organizations. The following overview was performed without access to official sources. However, critical assessment is difficult when one is devoid of a shared factual base.

In 2010, the US DoD's decision to lift the self-imposed taboo on speaking about cyber-offense probably helped the IDF to state in 2012 that it was considering offensive cyber-warfare. In August 2015, the Israel Defense Forces (IDF) published its first formal defense doctrine, authored by IDF Chief of General Staff Lt. Gen. Gadi Eizenkot. The publication of the unclassified version of the IDF Strategy document formulated within the framework of the "Gideon" multi-year plan was a significant progress in civil-military relations. While not a binding document, the IDF Strategy outlined the military's view of strategic and operational responses to the main threats facing Israel and asked the political echelon for clearer instructions. The IDF Strategy outlined the principle to operate the force in contexts that are common to all operational theaters against a semi-state enemy and in the IDF's various functional situations: Routine, Emergency, and War.

Conceptualisation of Cyberdefense as Mabam

The 2002, 2006, 2008-09, 2012, and 2014 rounds of large-scale violence demonstrate IDF's missions in the twenty-first century. The IDF developed the "campaign between wars" concept (*Mabam – Maaracha bein Milhamot*) to describe the military operations short-of-war, which IDF initiates and performs to thwart emerging enemy threats. This became an official doctrinal term later and was included in the summer 2015 IDF Strategy document. These covert and overt operations range from remote or on-the-ground intelligence collection, to surgical Special Forces raids, to precision strikes and to brigade-level combined arms maneuvers. The use of force is not intended to attain political goals, but rather to debilitate the capabilities of the enemy to harm Israel. For example, the range of strikes against Iranian forces in Syria and elsewhere often targeted weaponry shipments, key persons, or installations.

The *Mabam* concept appears to serve cybersecurity well. Mature cyber defense no longer singularly aims to prevent a breach. Nowadays, two models—the cyber kill chain and defense-in-depth—guide effective cyber operations. *Mabam* is an almost-routine emergency, which does not lend itself to a single-blow battlefield victory. Mature cyber defense similarly perceives the reality as an ongoing, long-term, adversarial competition. Advanced cybersecurity experts never promise complete defense, let alone a decisive victory. The goal is to minimize the threat through defense in-depth, intelligence and pre-emptive actions. The *Mabam* concept also accepts the less-heroic operational routine rather than decisive victory that destroys the adversary.

Whether the IDF at large or any of the stakeholders (C4I or Intelligence) consider cybersecurity on such terms is highly unclear.

Conceptualisation of Cyberdefense as Air Dominance

This overarching quality-over-quantity strategy has led the IDF to a long record of operational accomplishment against the Arab states that practised military aggression. As a result, Egypt and Jordan have signed peace treaties and Assad's Syria has not fired a shot at Israel since 1982. These and other factors have led to the strengthening of the Air and Intelligence branches within the IDF.

The Air Force enjoys complete dominance and can operate against any ground, air, or naval target in the broader Middle East. The IAF became both the long strategic arm as well as the main contractor of precision fire, replacing the Artillery. This air dominance, of course, depends largely on the advanced exploitation of ICTs—cyber technologies—in all phases: planning; logistics; intelligence collection, analysis, and dissemination; C2; EW; defense suppression.

What would be the operational, strategic, and political benefits to the IDF if it aimed to assure cyber dominance? Inevitably, this would lead to drastic change. Much of cybersecurity practice seeks to minimize risks to the existing ways of “doing business.” If your theory of victory rests on dominant armored maneuver, then you would need cybersecurity only as much as it can support operating armor units. If your theory of victory rests on manipulating the adversary's political decision-making process and calculus by means of persistent influence operations inter alia via Social Media, then cybersecurity would have a qualitatively different role.

The Way Forward

For modern developed nations in general and for Israel, in particular, the national military have proven to be the most successful defense organization that provides security vis-à-vis other states. But, can militaries secure our societies from foreign cyber threats? To assume so is far from certain. Israel's defense expenditure ranges between 5% to 6% of its GDP – roughly four times the average of Western democracies. How much of this contributes to national civilian cybersecurity? Israel's National Cybersecurity Strategy accepts the division of responsibility between defense and civilian sectors: The Resolution 3611 does not

apply to “Special Bodies:” the Israel Defense Forces, the Israeli Police, Israel Security Agency (*Shabak*), the Institute for Intelligence and Special Operations (*Mossad*) and the defense establishment (mainly the defense-industrial base). The Directorate for Security of the Defense Establishment (*Malmab*) in the Ministry of Defense will remain the government’s regulator for the cybersecurity of the defense sector.

The MoD and the IDF do not undertake the mission to defend the entire society in cyber. The defense sector defends itself in cyber, while the new national civilian organization has been established to cater for all the rest. Such a division is common to all Western democracies. Western militaries in general and the IDF, in particular, play an almost negligible role in providing national cybersecurity for their societies. Western military leaders must first face this reality and form a position on the desired military role in national cybersecurity. The range of options to enhance national cybersecurity can be derived from two general strategies:

- Get the militaries to provide more cybersecurity. This requires re-balancing between security and basic liberties so that Armed Forces could act within domestic civilian cyberspace
- Provide more cybersecurity without the militaries. This requires slashing conventional defense forces to free up resources for cybersecurity and establishing new civilian organizations.

Defense thinkers and leaders must invest major efforts in devising effective national cybersecurity, which will require radical innovation within defense establishments and elsewhere. Israel has been innovating with cybersecurity policies since 2002. While Israel has achieved relative success in civilian cybersecurity, more innovation is to be expected.

Disclaimer

The views expressed are solely those of the contributing author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium’s editors.

About the Author

Dr. Lior Tabansky is Head of research development, The Blavatnik Interdisciplinary Cyber Research Center of Tel Aviv University. Lior Tabansky offers a unique cybersecurity grasp, combining academic research in International Security Studies, 15 years of IT-pro work and business experience in formulating cyber strategies. Mr. Tabansky's 2015 book *Cybersecurity in Israel*, co-authored with Professor Isaac Ben-Israel, is the first comprehensive "insider" account of decades of Israeli policy and operations. Moreover, the book develops an original analysis of the roles grand strategy and innovation play in cybersecurity. Lior's doctoral dissertation reveals why even the most developed nations remain so exposed to destructive cyberattacks on strategic homeland targets by foreign states.
E-mail: cyberacil@gmail.com.



Cybersecurity in Switzerland: Challenges and the Way Forward for the Swiss Armed Forces

Marie Baezner

Center for Security Studies, ETH Zurich

Abstract: The cybersecurity policy of Switzerland is focused on enhancing competencies and knowledge, investing in research and the resilience of critical infrastructures, threat monitoring, supporting innovation, promoting standards, and increasing awareness – all in the framework of public-private, inter-regional, and international cooperation. The armed forces support this policy by developing threat intelligence and attribution capabilities, readiness to undertake active measures in cyberspace, and to ensure operational availability under any circumstances.

Keywords: cyber risks, cybersecurity strategy, resilience, crisis management, law enforcement, cyber defence, cyber operations.

Policy Highlights

Like in any other European state, cybersecurity has grown in importance in Swiss politics. And although Switzerland's cybersecurity and defense policies are still a work in progress, the nation has made tremendous efforts in getting cybersecurity policies, roles, and responsibilities right.

Published in 2018, the "National Strategy for the Protection of Switzerland against Cyber Risks"¹ is the main policy document that guides Swiss ambitions and replaced the 2012 strategy.² Overall, the strategy sets seven strategic goals

¹ Swiss Federal Council, *National Strategy for the Protection of Switzerland against Cyber Risks (NCS) 2018-2022* (Bern: Federal IT Steering Unit FITSU, April 2018), https://www.isb.admin.ch/dam/isb/en/dokumente/ikt-vorgaben/strategien/ncs/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_EN.pdf.

² Federal Department of Defense, Civil Protection and Sport DDPS, *National Strategy for the Protection of Switzerland against Cyber Risks* (revised), June 2012,

and ten spheres of action. The goals can be summarized as preparing Switzerland to face the cyber risks of tomorrow head-on, by building up cybersecurity competencies, crisis management structures, strengthening resilience, and facilitating international cooperation.

The strategy is accompanied by an implementation plan,³ which was the result of three consultations with the main stakeholders in the Swiss cybersecurity landscape. While the steering of the strategy is centrally organized, its implementation is decentralized with a clear distribution of roles. The implementation plan sets out specific measures to implement the ten spheres of action defined in the 2018 strategy. It also clarifies responsibilities, outlines quantifiable objectives, and maintains a schedule to evaluate implementation progress.

The Swiss Reporting and Analysis Centre for Information Assurance (MELANI) is the institution responsible for writing and implementing the strategy, and informing the Swiss population and the private sector on any new cyber threats.

Another important document is the *Cyber Defense Action Plan 2017* for the Federal Department of Defense, Civil Protection and Sport (DDPS). The Action Plan defines the role of the DDPS, the Federal Intelligence Service (FIS), and the armed forces within the Swiss cybersecurity landscape. Overall, their role is to protect the DDPS' networks and critical infrastructures from cyber threats, conduct military and intelligence cyber operations, and support civilian critical infrastructures in case of a major cyberattack.

The Swiss political landscape has undergone considerable changes during the past few years. In 2016, the Federal Council published its report on Swiss security policy,⁴ which underlined the risks caused by information technologies and the changing nature of conflict with regard to cyberspace. The Swiss Parliament passed a new intelligence law, which came into force in 2017,⁵ and the military law⁶ was revised in 2018 to allow the armed forces to have the means to protect their networks and conduct offensive cyber countermeasures. The Federal Council also recently launched a Federal Council Cyber Committee as a driver for in-

<https://www.isb.admin.ch/dam/isb/en/dokumente/ikt-vorgaben/strategien/ncs/Strategie%20zum%20Schutz%20der%20Schweiz%20vor%20Cyber-Risiken.pdf>.

³ Swiss Federal Council, "Implementation Plan for the 2018-2022 National Strategy for the Protection of Switzerland Against Cyber Risks (NCS)," May 2019, https://www.isb.admin.ch/dam/isb/en/dokumente/themen/NCS/Umsetzungsplan_NCS_2018-2022_EN.pdf.

⁴ "Die Sicherheitspolitik der Schweiz: Bericht des Bundesrates," August 24, 2016, <https://www.vbs.admin.ch/de/themen/sicherheitspolitik/sicherheitspolitische-berichte/sicherheitspolitischer-bericht-2016.detail.document.html/vbs-internet/de/documents/sicherheitspolitik/sipolb2016/SIPOL-B-2016-de.pdf.html>.

⁵ "Federal Act on the Intelligence Service (Intelligence Service Act, IntelSA)," September 25, 2015 (status as of March 1, 2018) <https://www.admin.ch/opc/en/classified-compilation/20120872/index.html>.

⁶ "Bundesgesetz über die Armee und die Militärverwaltung (Militärgesetz, MG)," February 3, 1995 (Status as of Januar 1, 2020), <https://www.admin.ch/opc/de/classified-compilation/19950010/index.html>.

creased centralization in the cybersecurity sphere, which is unusual for Switzerland. As a federal state, the preference is to leave a certain leeway to the 26 cantons and the private sector. The Cyber Committee is also in charge of monitoring the implementation of the national cybersecurity strategy.

These political developments show that the Swiss government takes cybersecurity issues seriously by treating them at the highest political levels. The Federal Council has also created a Cyber Security Competence Centre, which functions as a single point of contact for all cybersecurity issues at the national level. It also coordinates the implementation of the national strategy. Finally, the latest development has been the nomination of a delegate for cybersecurity who not only steers the cybersecurity strategy but also heads the special federal committee on cybersecurity and represents the Swiss Confederation in other committees.

Policy Challenges

The National Strategy for the protection of Switzerland against cyber risks tackles a broad set of cybersecurity issues. As such, it encompasses the development of technical capabilities, streamlining education, fighting cybercrime, strengthening the military, increasing international cooperation, and raising awareness. While the strategy is specifically focused on cybersecurity, it also naturally aligns with Switzerland's national security policy of 2016, the Federal Council's strategy for a digital Switzerland 2018, the national strategy on critical infrastructure protection 2018-2022, and integrates the recent changes in the intelligence and the military law.

Overall, the strategy underlines the necessity of developing public-private partnerships and closely engaging with the private sector on the one hand and insists on the subsidiary role of the state on the other. With regard to the armed forces, the strategy mentions the need to develop defensive capabilities but also to ensure the armed forces' ability to undertake active measures in cyberspace. These active measures are understood as ways and means to disturb, prevent, or slow down an adversary targeting Swiss critical infrastructure. Additionally, the strategy also specifies that Switzerland has an active role to play in shaping cyber norms at the international level and cooperate with other nations. Finally, the strategy underlines the importance of raising public awareness of cybersecurity issues. The strategy covers all of these elements in the following ten spheres of action:

1. Building competencies and knowledge
 - Measure 1: monitoring of trends in technological innovations
 - Measure 2: improvement of the research and education in cybersecurity
 - Measure 3: establishment of frameworks that would encourage innovation in cybersecurity
2. Threat landscape

- Measure 4: improvement and extension of capabilities in analysis and presentation of the cyber threat landscape
- 3. Resilience management
 - Measure 5: improvement of the resilience of critical infrastructures
 - Measure 6: improvement of the resilience of the federal administration networks
 - Measure 7: improvement of the resilience of cantons' networks through information and experience sharing
- 4. Standardization/Regulation
 - Measure 8: definition and introduction of minimum standards to improve network resilience
 - Measure 9: start of a review on an obligation to report cyber incidents
 - Measure 10: more involvement of Switzerland in international governance of the Internet to ensure the development of a free and democratic Internet
 - Measure 11: establishment of expert groups to evaluate regulations regarding cybersecurity
- 5. Incident management
 - Measure 12: development of MELANI as a Public-Private Partnership
 - Measure 13: offering MELANI services to all types of enterprises
 - Measure 14: development of the collaboration between the Swiss government and other centers of competence
 - Measure 15: establishment of a process to clearly define responsibilities in cyber incident management within the federal administration
- 6. Crisis management
 - Measure 16: integration of cyber experts in crisis management cells to foster collaboration with the private sector, if needed
 - Measure 17: organization of joint exercises in crisis management with the integration of cybersecurity elements in larger exercises and the organization of cyber-specific exercises
- 7. Prosecution
 - Measure 18: establishment of a table of the current cybercrime violations in Switzerland
 - Measure 19: enhancement of the collaboration between the various competence centers and the national network of investigators specialized in cyber criminality

- Measure 20: development of the education for law enforcement to build knowledge regarding the prosecution of cybercriminal cases
 - Measure 21: modification of the current structure of federal offices in charge of criminal affairs to establish a new Central Office on the fight against cyber criminality to enhance collaboration among cantons in cases of cyber criminality
8. Cyber defense
- Measure 22: development of threat intelligence and attribution capabilities
 - Measure 23: ensuring the armed forces' abilities to undertake active measures in cyberspace in accordance with the new legal basis
 - Measure 24: development of the armed forces to ensure their operational availability in all circumstances
9. Active positioning of Switzerland in international cybersecurity policy
- Measure 25: involvement of Switzerland in early discussions in international forums concerning cybersecurity
 - Measure 26: enhancement of international cooperation to improve capabilities and information sharing in cybersecurity
 - Measure 27: establishment of bilateral and multilateral dialogs on foreign security policies regarding cybersecurity
10. Public impact and awareness-raising
- Measure 28: implementation of a communication strategy for the strategy
 - Measure 29: raising awareness in the public about cyber risks.

The ten spheres of action and the enclosed measures mostly seek to develop existing structures and fill the gaps that have been identified in the 2012 national strategy. The main differences between the 2018 and 2012 strategy concern three spheres of action. The first difference concerns crisis management and awareness-raising. In the 2018 strategy, the population, small and medium enterprises, and cantons have been included among the target groups, while in the 2012 strategy, the focus was only on critical infrastructure operators. The second difference refers to the standardization and regulation. The 2018 strategy mentions an examination of a possible obligation to report cyber incidents and the evaluation and introduction of minimum standards for IT security in critical infrastructure. These new measures echo the European Union Network and Information Security (NIS) directive. The third difference relates to cyber defense. The 2018 strategy includes the armed forces' role and responsibilities while they were almost totally absent from the first strategy.

Similar to the National Strategy for the protection of Switzerland against cyber risks, the Cyber Defense Action Plan (PACD) 2017 recognizes the need for a comprehensive approach to cybersecurity. The PACD 2017 acts as a roadmap

for the DDPS to reinforce its cyber capabilities. The document seeks to highlight lessons learned from the RUAG cyberattack in 2016⁷ and national cyber defense exercises. The PACD 2017 identifies five major fields in which the DDPS needed to make progress: strategic management, developing operational means, building support from the militia structure, improving collaboration with higher education and the private sector, and finding the workforce. The PACD 2017 mentions that since 2016 the DDPS has already started to take measures such as implementing an Information Security Management System (ISMS) according to the ISO 27000 series of standards and modernizing its systems and network infrastructure. The PACD 2017 is very transparent about the resources it needs to achieve its objectives.

Policy Implementing Structures and Whole-of-Nation Context

Switzerland is one of the most federalized and decentralized countries in the world. A large number of tasks are left to the cantons to manage, including education and law enforcement. This decentralization is sometimes perceived as a challenge and/or restriction for the federal government to tackle new issues like cybersecurity. Actually, the past years have shown that the trend on the issue of cybersecurity has been a move toward more centralization at the federal level.

Coordination structure. With the new strategy, Switzerland has set up a new overarching structure with the Federal Council Cyber Committee, the cyber security delegate, and the Cyber Security Competence Centre. All these new institutions play a role in the coordination of cybersecurity at the federal level:

- *Federal Council Cyber Committee:* The Committee is composed of the heads of the Federal Department of Finance, the DDPS, and the Federal Department of Justice and Police (FDJP). The Committee meets four times a year and its role is to monitor the implementation of the national cybersecurity strategy;
- *Cyber Security Delegate:* The Federal Council is responsible for choosing the Cyber Security Delegate. The Delegate is responsible for steering the agenda of the Swiss Confederation at the federal level regarding cybersecurity issues. The Delegate heads internal committees on cybersecurity and represents Switzerland in other committees in Switzerland;
- *Cyber Core Group:* The group reports to the Federal Council Cyber Committee and is responsible for enhancing the collaboration between the three sectors: cybersecurity, cyber defense, and criminal prosecution. The group is in charge of ensuring a joint threat assessment and super-

⁷ In January 2016, the Swiss media revealed that the technology firm owned by the Swiss Confederation had been targeted by a cyberespionage campaign attributed to the APT group Turla. For more information on this cyberattack, see: "APT Case RUAG," GovCERT.ch, Technical Report, May 23, 2016, <https://www.melani.admin.ch/dam/melani/en/dokumente/2016/technical%20report%20ruag.pdf>.

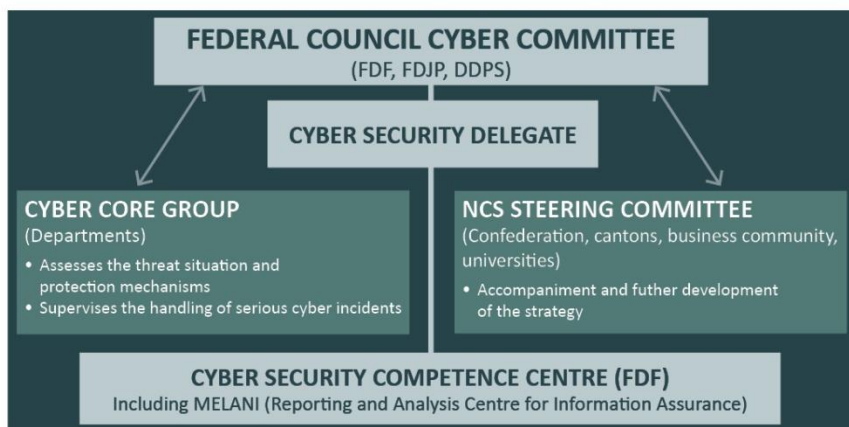


Figure 1: Federal Cyber Risk Organization.

vises through federal entities the management of cyber crises involving several Federal Departments;

- *NCS Steering Committee*: The Committee reports to the Federal Council Cyber Committee and ensures that the implementation of measures from the strategy stays coordinated. The NCS Steering Committee also helps with suggestions for further policy developments;
- *Cyber Security Competence Centre*: The Centre is subordinate to the Federal Department of Finance and includes MELANI. The Centre is the single point of contact for cybersecurity issues at the federal level and ensures the coordinated implementation of the strategy.

Military roles and responsibilities: The armed forces are part of the DDPS. Their role is to protect and defend their own networks and critical infrastructure against cyberattacks, to support the FIS in responding to cyberattacks targeting civilian critical infrastructures, and to maintain capabilities in cyberspace in case of war. The conditions for the armed forces to support the FIS in defending against cyberattacks are very strict and the armed forces would only be involved as additional help. The Electronic Operations Centre (EOC) is the main actor for military cyber defense in the DDPS. The EOC is responsible for fulfilling the aforementioned tasks and collaborates with the FIS with regard to critical infrastructure. The EOC is composed of military and civilian personnel, the military conscripts working at the EOC report to the Command Support Brigade 41. With the revision of the military law, the armed forces can now conduct offensive cyber countermeasures with the authorization of the Federal Council.

Law enforcement role and responsibilities:

- *Cantonal police forces*: Fighting cybercrime or cyber-enabled crimes is the role of cantonal police forces. Each canton allocates resources and organizes its fight against cybercrime as it desires. The Canton of Zurich built a Cyber Security Center and is one of the cantons that invests the most in fighting cybercrime. On the other hand, smaller cantons have more limited resources and may not be able to build centers like in the Canton of Zurich. Cantonal police forces coordinate and exchange information on cybercrime in various national platforms such as the Swiss Conference of Chiefs of Cantonal Police, the Conference of Directors of Cantonal Departments of Justice and Police, the Swiss Security Network or the newly created Cyberboard, whose role it is to keep an overview on the cybercriminal violations in Switzerland;
- *Federal Police (Fedpol)*: Fedpol is responsible for fighting organized crime, coordinating relations with foreign police forces, protecting people and buildings under the responsibility of the Swiss Confederation, and coordinating the identification processes (e.g., passports, IDs, immigration). Regarding cybercrime, Fedpol is only responsible for investigating cybercrime cases that fall under the jurisdiction of the Swiss Confederation (i.e., cybercrime linked to the areas of responsibilities mentioned above);
- *Office of the Attorney General of Switzerland*: The Attorney General is in charge of prosecuting cybercriminal cases that fall under the jurisdiction of the Swiss Confederation.

Intelligence role and responsibilities: The Federal Intelligence Service (FIS) is in charge of the counterintelligence and attribution, supports critical infrastructures targeted by cyberattacks, fights against terrorism in cyberspace, and conducts awareness-raising campaigns about cyber espionage. Until 2017, the FIS was limited to defensive measures in cyberspace. With the new law, the FIS has the legal basis to conduct offensive cyber countermeasures against infrastructures located outside Switzerland after authorization by the head of the DDPS who needs to confer with the heads of the FDFA and the FDJP first.⁸

Federal Department of Foreign Affairs (FDFA) role and responsibilities: The Security Policy Division of the Federal Department of Foreign Affairs is responsible for diplomatic measures like participating in international forums about cybersecurity norms, the development of international treaties on cybersecurity issues and Internet governance.

Policy Implementation

International cooperation: While Switzerland is neutral, it does not refrain from cooperating bilaterally or multilaterally with other countries. Switzerland has

⁸ Article 37 of “Federal Act on the Intelligence Service,” September 25, 2015, <https://www.admin.ch/opc/fr/classified-compilation/20120872/index.html#a37>.

shown that it is aware that cybersecurity issues cannot be tackled alone. Regarding cybersecurity, Switzerland mainly collaborates through its intelligence service, its armed forces, and the FDFA. Since 2019, Switzerland is also a contributing partner of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn. This partnership allows Switzerland to access knowledge, information, and training but also to participate in various activities offered by the CCDCOE.⁹ Switzerland already took part in various international exercises such as Locked Shields, Crossed Swords, Cyber Coalition, Cyber Storm, and Cyber Europe. Switzerland also collaborates and exchanges regularly with its neighbors and other states regarding cyber threat intelligence and practices.

Through the FDFA, Switzerland is involved internationally to promote the development of international cyber norms in organizations like the UN and the OSCE. Switzerland participates in the United Nations Governmental Group of Experts (UN GGE) and chairs the Open-ended Working Group (OEWG). Switzerland wants to contribute to the discussion on the respect and application of international law in cyberspace and to establish trust among states regarding cybersecurity issues. Finally, Switzerland promotes itself and Geneva as a discussion platform for cybersecurity issues.

Engagement of private sector/NGOs/academia: In 2018, the DDPS launched the Cyber Defense Campus (CYD Campus), whose role is to serve as a research and development hub connecting the armed forces, academia, and the private sector. The CYD Campus is part of Armasuisse, the Federal Office for Defense Procurement, located in the DDPS. The CYD Campus is developing offices at the EPFL in Lausanne and the ETH in Zurich. The objective is to be as close as possible to startups and innovation, to monitor new technologies and talents, to do research, and to train talents.¹⁰ The CYD Campus should reach its full capacity by the end of 2020.

The DDPS also collaborates with the Swiss Academy of Engineering Sciences (SATW) to map research and development projects on cybersecurity in Switzerland. Additionally, DDPS assigned research projects on technical and non-technical topics linked to cybersecurity to higher education institutions.

Finally, the DDPS supports cyber competitions such as the 9/12 Strategy Challenge organized by the Geneva Centre for Security Policy (GCSP) and the Swiss Cyber Storm, to promote the field of cybersecurity and to find talents.

Conscription army: In August 2018, the Swiss armed forces launched a cyber defense training program for conscripts. The training program has the long-term

⁹ "Participation au Centre d'excellence pour la cyberdéfense en coopération," May 22, 2019, <https://www.admin.ch/gov/fr/accueil/documentation/communiqués.msg-id-75145.html>.

¹⁰ "Cyber-Defence Campus," https://www.ar.admin.ch/fr/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus.html.

objective to train 600 conscripts to become cybersecurity specialists that will be integrated into a cyber defense battalion.¹¹

The Way Forward

Because cybersecurity issues will continue to be significant challenges for states, Switzerland should continue with its recent developments and improvements that started during the past three years. Switzerland's latest initiatives and policies relating to cybersecurity are new and it is still too early to evaluate and notice their effects. Time will tell if these measures will help Switzerland to face the cybersecurity challenges of tomorrow. However, recent measures will remain important for Switzerland in the coming years. International cooperation will remain significant because of the cross-border nature of cybersecurity. These challenges cannot be tackled alone and, therefore, Switzerland should continue to cooperate bilaterally and multilaterally. The cyber defense training program will regularly bring conscripts in the future cyber defense battalion. These new cybersecurity specialists will contribute to building capabilities and would benefit first the Swiss armed forces but also the whole society when they go back to their civilian life. Overall, Switzerland should continue its momentum and carry on with the implementation of its strategy and the buildup of its capabilities in the military and civilian institutions.

Disclaimer

The views expressed are solely those of the contributing author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

About the Author

Marie Baezner is a Researcher in the Cyber Defense Team of the Center for Security Studies. She holds an MA in International Security from the University of Bath, United Kingdom, and a BA in International Relations (Political Science and International Law) from the University of Geneva. Before joining the CSS, Marie Baezner has worked for the Command Support Basis of the Swiss Armed Forces and the Swiss Armed Forces Peace Support Mission in Kosovo. Marie Baezner's research focuses on cyber incidents and cyber aspects of current conflicts. E-mail: marie.baezner@sipo.gess.ethz.ch.

¹¹ "Premières expériences dans le domaine de l'instruction en cybernétique," <https://www.vtg.admin.ch/fr/armee.detail.news.html/vtg-internet/verwaltung/2018/18-09/erste-erfahrungen-mit-dem-cyber-lehrgang-der-armee.html>.



Research Article

National Cyber Security Strategy and the Emergence of Strong Digital Borders

Sanjay Goel

New York State Center for Information Forensics and Assurance, University at Albany, 1400 Washington Avenue, Albany, NY 12222

<https://www.albany.edu/cifa/>

Abstract: The growth of the Internet and innovation that thrived with it was facilitated by an environment relatively free of controls. Regrettably, however, with its deep integration into the societal framework, the Internet has become a potent tool for influencing geopolitical conflicts, including interference in internal affairs of other nations, undermining national security, destabilizing financial infrastructure, and attacks on critical infrastructure. While countries are harvesting the social and economic benefits of the Internet, they are frightened of the threats it poses to national security. In response to these threats, countries are starting to tighten their internet borders and developing their cyber weaponry both as a deterrent to, and leverage during conflicts. A potential downside of such state-by-state regulation is inhibition of the rapid innovation that the Internet has traditionally fostered and the curtailing of freedom of speech that has led to the social integration in the society. On the other hand, innovation and freedom cannot thrive in a chaotic environment with rampant crime and a lack of rules, norms, and ethics. With this in mind, national policymakers face the challenge of striking a balance between regulation and potential chaos on the Internet while at the same time promoting freedom. In efforts to strike such a balance of national interests, borders in cyberspace have an important role to play along with international efforts to build trust in cyberspace and to slow down the fragmentation of the Internet. This article discusses how cyber conflicts are escalating, how mutual distrust is growing, and how nation-states are adapting to the constantly changing cyber domain.

Keywords: Cyber threats, critical infrastructure, cyber conflict, international law.

Introduction

Sophistication and impact have continuously escalated since the first Morris worm cyberattack in 1988¹ and have recently become a key part of national defense strategies of several countries. Cyber is now considered a separate domain of conflict along with land, sea, air, and space, clearly indicated in military doctrines of the strongest nations in the world, i.e., Russia, China, and the US. Each country is shoring up their defenses and, at the same time, working furiously to develop cyber weapons and probe the cyber defenses of other countries. Cyberattacks have already been used to complement military interventions, retaliate against the policies and actions of other countries, and to interfere in the elections of other countries. A fierce cyber arms race has ensued with no signs of abatement. Nation states now face a dilemma on whether to work cooperatively to de-escalate the cyber arms race and allow the Internet to prosper unfettered, or to put borders on the Internet and threaten its growth and evolution.

There have been several attempts at treaty formation for containing the growth of cyber weaponry; however, lack of attribution, increasing vulnerabilities, escalation in economic rivalries among nations are making consensus building around these treaties hard. While attribution around cyber incidents is getting better based on improved analytic techniques, the development activities of nations around cyber weapons are still sheathed. A game-theoretic view of the situation suggests that each country needs to keep maximizing its cyber arsenal, assuming that other countries are maximizing their efforts at developing cyber arsenals. The earliest cases of cyber warfare occurred in conflicts between Russia and the former Soviet republics of Georgia and Estonia. In those cases, attacks were used for media propaganda, defacement of websites, etc. Over time, however, cyberattacks are becoming more sophisticated, targeted, and dangerous. Also, more nation states are embracing cyberattacks and using the attacks strategically to meet their geopolitical objectives.

This article frames the current challenges and discusses the potential outcomes of this conflict. In section 2 it lists key incidents over the last two decades that show the escalation of the sophistication and impact of nation-state cyberattacks. Section 3 discusses how the future evolution of the Internet exponentially increases the threat landscape. Section 4 discusses how countries are reacting to the escalation of cyber threats by tightening Internet borders and launching a regime of monitoring and censorship within their borders. Section 5 discusses international efforts at building trust and cooperation in cyberspace to avoid the balkanization of the Internet and to slow down the cyber arms race.

¹ Craig Timberg, "Net of Insecurity: A Flaw in the Design," *The Washington Post*, May 30, 2015, accessed August 13, 2018, <https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1>.

The Evolution of Cyber Warfare

Operation Aurora, originating from China in 2006, is a targeted malware attack against at least 30 major companies—including Google and Adobe—which exploited a zero-day flaw in Internet Explorer. The exploit allowed malware to load onto users' computers. Hackers seem to have accessed the source code for numerous software products. Five members of Unit 61398 of the People's Liberation Army were "assigned" to deploy a widespread spear-phishing (or "spearfishing") campaign to allegedly hack into leading US companies. The attack involved breaches at 141 companies spanning 20 major industries from 2006 to 2014. Hackers went after American trade secrets: from Westinghouse, for example, the hackers are alleged to have taken plans for a certain type of nuclear power plant. This was the first time the term "advanced persistent threat" was coined.

Stuxnet, discovered in 2010, was a worm that some researchers suggest was developed by the United States and Israel for targeting the Iranian nuclear program by infecting the programming logic controllers (PLCs) of the centrifuges in Iranian reactors. It is thought that the malware may have been introduced through thumb drives of nuclear inspectors sent to Iran through the IAEA. The malware destroyed the centrifuges by changing their rotational speeds beyond their range of operations.

Operation Cleaver, originating from Iran in 2012, conducted a significant global surveillance and infiltration campaign, including the US Navy. It successfully evaded detection and leveraged common tools to attack and compromise targets around the globe. The targets included military, oil and gas, energy and utilities, transportation, airlines, airports, hospitals, telecommunications, technology, education, aerospace, Defense Industrial Base (DIB), chemical companies, and governments. The attack resulted in the theft of sensitive information or took control of critical infrastructure networks in many countries, including Canada, China, England, France, Germany, India, Israel, Kuwait, Mexico, Pakistan, Qatar, Saudi Arabia, South Korea, Turkey, the United Arab Emirates, and the United States.

OPM Attack. The office of Public Management (OPM) attack started in March 2014, targeting US government data and leading to the theft of over 21 million data records. The hack compromised personal information (social security numbers, dates of birth, addresses, etc.) and detailed security-clearance-related background information. Attackers gained valid user credentials to the systems they were attacking, likely through social engineering. The breach involved installation of a malware package within OPM's network and established a backdoor. From there, attackers escalated their privileges to gain access to other OPM systems and data.

DNC Breach. During the 2016 US elections, an attack was orchestrated from Russia to the email servers for the Democratic National Committee (DNC) and the Gmail account for Clinton campaign chairman John Podesta. At least 60,000 emails were stolen and subsequently published by Wikileaks, leading to the res-

ignations of top officials and a major embarrassment for the DNC and the Clinton Campaign.

NotPetya. In 2017, the malware NotPetya spread from the servers of an unassuming Ukrainian software firm to some of the largest businesses worldwide, paralyzing their operations. Some of the damages of major corporations included Merck, which lost 870 million, FedEx, which lost 400 million, Saint-Gobain, which lost 384 million, and Maersk, which lost 300 million, with a total loss of over 10 billion dollars. It is suspected that the attack was launched at the behest of the Russian military.

Each of these attacks represents a clear political objective, i.e., interfering in elections, causing economic impact during conflict, retaliation against an attack, and gathering military intelligence. The ramifications of the attacks are becoming more and more dangerous, and the adventurism of countries continues to increase. Countries are resorting to cyber attacks instead of conventional attacks due to the nebulous attribution and less fear of international condemnation. The stakes are going to get even higher as cyber-physical systems mature and gain mainstream acceptance in society, i.e., self-driving cars, implantable and wearable devices, and smart metering. These ramifications are discussed in the next section.

The Expanding Vulnerability Landscape

Three major innovations of this decade are the smart grid, connected vehicles, and human implantable devices. All three will radically transform society in many ways, some of which cannot be currently conceived. A lot of the discussion around cyber-physical systems is very timely, as the implications of cyber-physical systems on the future of society are enormous.

We are creating three classes of networks: a monolithic network of devices and sensors on the power grid; millions of ad hoc networks in the traffic grid; and a huge personal network in wearables. There are massive challenges in each of them. Most of the discussion here has been pertinent to the static networks of cyber-physical systems such as industrial control, power, and gas distribution. What we have not addressed are the constantly changing networks of connected vehicles and wearable technologies. Let us take a closer look at IOT evolution.

Gartner has estimated that there will be 21 billion employed IoT devices within the next couple of years. Cisco is estimating 50 billion devices, and Intel is taking it further, with a prediction of 200 billion IoT devices.² And truly, we are just beginning to understand the potential and promise of the Internet of Things. The range of possible benefits is expanding as adoption increases, with greater efficiency, streamlined processes, and reduced costs being top benefits realized

² Nathan Eddy, "Gartner: 21 Billion IoT Devices to Invade By 2020," *Information Week*, October 11, 2015, accessed April 11, 2018, <https://www.informationweek.com/mobile/mobile-devices/gartner-21-billion-iot-devices-to-invade-by-2020/d/d-id/1323081>.

by all manner of business enterprises. The first revolution came with the creation of the power loom (1784). The second industrial revolution came with the assembly line (1870), and the third industrial revolution came with PLCs (1969). The fourth revolution is happening now and is being driven by sensors, Artificial Intelligence (AI), and robotics.

Imagine for a moment smart farming and the advances in production and prediction that will be realized when sensors can deliver fine-tuned information about temperatures and humidity, soil pH and nutrient levels, to inform farming practices and increase crop yields. Or the remarkable potential in medicine and biomedical informatics of insulin pumps that can monitor blood sugar levels and adjust insulin levels *in real-time*, or IBM's Medical Sieve, which, driven by smart algorithms and advanced AI, sorts through a patient's complete medical history, looking for clues to inform its analysis of the patient's images; learning everything there is to know about the individual in seconds for a smarter diagnosis and an infinitely more personalized treatment plan.³

Imagine recapturing the time you currently spend fighting traffic on your daily commute, for reading or even daydreaming, in your self-driving vehicle. The University at Albany is working on a project where traffic signals can communicate with each other, making adjustments to increase traffic flow. Imagine sensors that can predict earthquakes *before* they happen; and the improvements that could be made with greater real-time energy consumption and environmental performance monitoring. IoT has transformed the world of energy generation and transformation. Today we are building an architecture of the power grid that will integrate multiple disparate power grids and make it more resilient. By overlaying a communication grid on top of the power grid and creating an information network that can connect sensors throughout the grid to make it resilient, an integrated electricity market is created where everyone can buy and sell electricity.

Today, 54% of people worldwide live in cities, a proportion that is expected to reach 66% by 2050. Combined with the overall population growth, urbanization will add another 2.5 billion people to cities over the next three decades. Rapid urbanization is causing severe environmental strain. Environmental, social, and economic sustainability must keep pace with this rapid expansion, which is taxing our cities' resources. The goal of smart cities is to promote sustainable development to manage urbanization challenges. By leveraging data efficiently from infrastructure and urban communities' own needs, cities can improve energy distribution, streamline trash collection, decrease traffic congestion, and even improve air quality with help from the IoT.

³ Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in *Proceedings of 2012 10th International Conference on Frontiers of Information Technology (FIT)* (Institute of Electrical and Electronics Engineers, December 2012), 257-260, <https://doi.org/10.1109/FIT.2012.53>.

How can we defend against hacking, cyber-attacks, and data theft? In cities where multiple participants are sharing information, how do we trust that participants are who they say they are? And how do we know that the data they report is true and accurate? With this unlimited promise comes tremendous risk in terms of security and privacy losses, system breaches, and hacking. When critical infrastructure, such as power stations, water supplies, airports, and hospitals, are governed by IoT systems, the potential for loss of life—from failures and cybercriminal activity—rises exponentially.⁴

The risks of IoT are not projections either; they are also here. According to a Hewlett Packard study, 80% of tested IoT devices (they tested commonly used home alarms and thermostats, garage door openers, etc.) raised privacy concerns, with an average of 25 security holes per device.⁵ In 2016, a DDoS attack—the largest in history—was launched on a service provider using an IoT bot with malware called Mirai, which led to huge portions of the Internet—including Twitter, Netflix, Reddit—going down. Mirai, once in, causes computers to continually search the Internet for vulnerable IoT devices and, using default usernames and passwords to initiate logins, infects them with Mirai also.

The security of our future—the IoT era—will only be as strong as the security of each of the billions of small connected devices that comprise our systems. We have all experienced a computer crashing and losing a document or a spreadsheet, but imagine a pacemaker or digitalized insulin pump that can be hacked, ending a life, or Volkswagen hacking their own cars to bypass emissions-control limitations. Imagine hackers gaining access to bank data and emptying accounts. Unauthorized personnel could access smart devices that store sensitive financial account information, passwords, and other information, exploiting these vulnerabilities to commit identity theft or fraud. A report published by the US Federal Trade Commission estimated that 10,000 households could generate 150 million data points daily, providing a significant number of entry points for hackers.⁶

Nation states are aware of these vulnerabilities and will seek to improve their leverage on other countries by exercising more sovereignty on the Internet. The concept of digital borders and Internet sovereignty has moved on from concept to actuality and several countries are working on controlling information flow across their borders as well as actively monitor and censor information within their border as we discuss in the next section.

⁴ Tianlong Yu, Vyas Sekar, Srinivasan Seshan, Yuvraj Agarwal, and Chenren Xu, “Handling a Trillion (Unfixable) Flaws on a Billion Devices: Rethinking Network Security for the Internet-of-Things,” in *Proceedings of the 14th ACM Workshop on Hot Topics in Networks* (ACM, November 2015), <http://dx.doi.org/10.1145/2834050.2834095>.

⁵ “HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack,” *HP News*, July 29, 2014, <https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676>.

⁶ Federal Trade Commission, “Internet of Things: Privacy and Security in a Connected World,” FTC Staff Report (January 2015), <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>.

Balkanization of the Internet

The Internet has operated with free access and international sovereignty for many years, allowing it to grow and develop into a ubiquitous communication platform that now also acts as a social glue for society and a platform for commerce and trade. One argument for opposing Internet restrictions is that information is an international human right. The more practical and economically powerful argument is that international trade is contingent on Internet access and cross-border data flows. The free and open access of the Internet is what made it very successful – but that success has also become its biggest challenge.

The Internet's enormous power in influencing public opinion and driving trade has made it a target for militarization. As US Defense Secretary Panetta observed, "the Internet is open. It's highly accessible, as it should be. But that also presents new terrain for warfare. It is a battlefield of the future."⁷ It is being used to influence public opinion and support regime change, to launch attacks on nation-states' information infrastructure, to recruit new members for terrorist organizations, and to disrupt and endanger critical infrastructure. What is unique about cyberspace (in relation to other physical domains like land, air, and space) is that it is global, but with a remarkably low cost of entry.

Propaganda and dissent have long been active forces in countries, but the sheer scale and reach of the Internet have made it a powerful weapon. Whether it is videos of protests or police brutality on YouTube, or new broadly effective Internet canvassing tools, the Internet is playing a powerful role in political organizing. Actors—even individual actors—can affect power in cyberspace that are orders of magnitude higher than what can be achieved by the small set of nations that operate with the consequence in the land, air, maritime, and space operational domains.

The Internet is a domain in which all other operational domains and national instruments of power are enabled (if not dependent). Given the tremendous power of the Internet, and in response to its use for political and military purposes, the concept of international Internet sovereignty is rapidly shifting towards the concept of sovereign Internet borders. This transformation is accelerating the pace of tightening Internet borders in recent years. Governments from China to Iran to Burma are increasingly filtering and blocking access to media and blogs that advocate political views that the government disagrees with.

The original and essentially libertarian nature of the Internet is increasingly being challenged by government assertions of jurisdiction over the Internet or the development of rules that restrict the ability of individuals and companies to access the Internet and move data across borders. The tools available for restricting access to the Internet and cross-border data flows are becoming increasingly available, complex, and broadly adaptable. These include blocking the backbone or access points into the country and the filtering of domain names,

⁷ Joshua P. Meltzer, "The Internet, Cross-Border Data Flows and International Trade," *SSRN Electronic Journal*, April 1, 2013, <http://dx.doi.org/10.2139/ssrn.2292477>.

Internet protocols, or URLs. Governments can also indirectly restrict access to the Internet by restrictive regulations that essentially limit search engines, for example by conditioning operating licenses on not posting particular material, and imposing stiff penalties for non-compliance. Control of information—for countries choosing to go that route—includes limiting access to foreign information sources, blocking foreign Internet tools such as Google search, Facebook, Twitter, and selected mobile apps, and requiring foreign companies to adapt to domestic regulations.⁸ However, as we put more and more controls in place, we are throttling the Internet and making it slower. The legitimacy of the government in enforcing national borders on the Internet comes from rules legislated ostensibly to protect citizens from deleterious external influence.

Let us look at the increasing Balkanization of the Internet, as some countries work to establish national boundaries while others fight for the Internet's original open-access internationalism. We will then look more closely at this dichotomy in the context of the growing militarization of the Internet and cyber warfare. Is it a false dichotomy, with even those countries—like the United States—advocating for a borderless Internet involved in cyber warfare and defense? Let us first examine the landscape of Internet borders – who is doing what?

Tightening Internet Borders for National Security

The emergence of the Internet in China has transformed the Chinese media from a closed and centralized system to an open and decentralized system. China has also seen a new population actively engaged on the Internet.⁹ By the end of 2017, China had 772 million Internet users, with a penetration rate of 55.8%, and had become the largest online population in the world. China has significantly expanded the technological capacity and human capital devoted to controlling Internet content, including employing an estimated 500,000-2 million Internet propagandists (more popularly known as 50cent army), to write the Internet comments to safeguard the prestige and integrity of the Chinese Communist Party.¹⁰

China, Saudi Arabia, Iran, and others have similar aspirations for the Internet: they think governments should get to decide what information flows across their borders, not companies and NGOs. A Freedom House 2018 report examined 65

⁸ Meltzer, "The Internet, Cross-Border Data Flows."

⁹ Wenfang Tang and Shanto Iyengar, eds., *Political Communication in China: Convergence or Divergence Between the Media and Political System?* (London: Routledge, 2012).

¹⁰ Tenzin Dalha, "Assertion of China's Sovereignty over the Internet," *global-is-asian*, October 4, 2018, <https://lkyspp.nus.edu.sg/gia/article/assertion-of-china's-sovereignty-over-the-internet>.

countries and found that since the previous year Internet freedom declined in 26 of them, with almost half of those declines related to elections.¹¹

China, as the architect of “cyber-sovereignty” has begun exporting its Internet censorship regime to other countries, changing the Internet from the bottom up. According to the Freedom House report, at least 36 governments (including Jordan, Egypt, Saudi Arabia, and Vietnam) have received closed-door Chinese training on “new media and information management.” For the past couple of years, China has hosted media officials from dozens of countries for two and three-week seminars on its censorship and surveillance system and supplied telecommunications hardware, advanced facial-recognition technology, and data-analytics tools to a variety of governments with poor human rights records. There is evidence that some countries, like Uganda, are using Chinese-made software to monitor their local Internets, ostensibly to fight crime.

Given broad-range global cyber incidents like NotPetya, interference in elections, and the insecurity that these incidents can sow, many countries are taking a more authoritarian approach to the Internet. A November 2018 cybercrime resolution backed by Russia and adopted by the UN General Assembly, saw three of the biggest democracies in the world—India, Brazil, and Nigeria—voting with Russia and China, clashing with more traditionally open countries including Australia, Canada, Estonia, France, Greece, Israel, the United States, and the United Kingdom. Late 2018 and early 2019 also saw the adoption of laws being passed or proposed that limit Internet freedoms in the name of mitigating vulnerability and combating cybercrime in Vietnam, Thailand, Egypt, the United Arab Emirates, and Tanzania.¹²

Russia’s government is tightening its control over the Internet, and Russia is not alone. In the lead-up to the 2018 election of Putin to his second term, authorities increased their already tight grip on the Internet blocking Telegram, the popular messaging service with over 10 million Russian users, because the platform refused to provide encryption keys to the FSB. There were protests against the legislative push to isolate Russia’s Internet by making it self-sufficient, supposedly to guard against external “threats.” Critics warn that the so-called “sovereign” Internet law will act as a sort of digital “iron curtain,” and serve as a tool for the government to impose censorship on dissenting views on social media. Reports suggest that Chinese and Russian-style paranoia about unrestricted online discourse is beginning to resonate in the West. Kieron O’Hara, a computer science professor and expert on Internet governance, says Western democracies

¹¹ Adrian Shahbaz, “Freedom on the Net 2018: The Rise of Digital Authoritarianism,” Freedom House, 2018, <https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism>.

¹² Justin Sherman, “How to Regulate the Internet Without Becoming a Dictator,” Foreign Policy, February 18, 2019, <https://foreignpolicy.com/2019/02/18/how-to-regulate-the-internet-without-becoming-a-dictator-uk-britain-cybersecurity-china-russia-data-content-filtering>.

are converging with China and Russia on common fears, leading to a shared affinity for something like an “authoritarian Internet” model.¹³

This tightening is not only an Eastern phenomenon—after interference in US presidential elections, there has been considerable debate on how to control propaganda on social media—which is a form of censorship. Internet media companies like Facebook and Google are being asked to take the lead in rooting out fake news from their websites. Some might see a big difference, though when one considers that the United States is attempting to root out false information, where some of the other countries are trying to root out genuine debate among its own citizens.

The economy and societies around the world are intricately woven with the Internet across the entire spectrum of society, including commerce, communication, education, and social relationships. The escalation of cyberattacks, interference in internal politics, and the potential for loss of lives and property should give nations pause. There have been several efforts to contain the cyber warfare arena through efforts to build cyber treaties and norms, as discussed below.

Diplomatic Brakes to De-escalate Cyber Arms Race

There is much debate on the norms and code of conduct in cyberspace. Ideally, the norms should focus on keeping a free flow of information on the Internet to empower people. However, the discussion has shifted to who, what and when there can be an attack on the Internet and the consequences of these attacks.

Three GGEs (Groups of Governmental Experts on Information Security) in the UN before 2016/2017 had established and carried forward an international conversation on cybersecurity since 2010, mainly on norms and confidence-building measures in cyberspace. The 2016/2017 group was tasked with determining “how international law applies to the use of information and communications technologies by states.” This issue—international law and its application—is a critical sticking point.

Authored by nineteen international law experts, the “Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations” was published in 2017, updating the 2013 analysis on how existing international law applies to cyberspace. It is notable that the new edition, just four years after, included a change in the book’s title referring to “cyber warfare” to “cyber operations;” a reflection that in today’s world cyberattacks usually fall well below the threshold at which international law would typically declare them to be a formal act of war.¹⁴

The OSCE has also been working on developing confidence-building measures (CBMs) for the last several years and has had some success in building consensus on preliminary points. The primary goal of these CBMs is to enhance transpar-

¹³ Eduard Saakashvili, “The Global Rise of Internet Sovereignty,” *.coda*, March 21, 2019, <https://codastory.com/authoritarian-tech/global-rise-internet-sovereignty/>.

¹⁴ Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

ency between states by promoting exchanges of information and communication between policy and decision-makers. The hope is that while these CBMs will not stop an intentional conflict, they can possibly mitigate an unintentional action by slowing down the escalation of events.

US's operational norms in air, land, and maritime domains are derived fundamentally from the concept of Westphalian sovereignty: "all members shall refrain in their international relations from the use of force against the territorial integrity or political independence of any state,"¹⁵ or responsible behavior should default to a pattern of operational restraint.

Without agreement on international law and its application to the cyber domain, including verification and attribution of incidents, many other aspects (including norms, confidence-building measures, and capacity-building) remain up in the air, as viewpoints seem to be diverging and solidifying rather than converging. One core question of the cyber domain is whether cyber operations—which most if not all countries engage in—follow a pattern of operational restraint or escalation.

Are Cyber Attacks Retaliatory or Strategic Actions by the Nation States

Are cyber operations primarily restrained? Are they meant to be escalatory or not? Are they effective as foreign policy instruments and maneuvers? Some would counter that the characteristics of cyberspace—including the uncertainty of effects and response, and the central lack of attribution and verification—seem, by their very nature, to be escalatory. But are they? One thrust to inform international policy is to understand better and quantify our present reality. A recent policy analysis paper from the Cato Institute looked at 272 documented cyber exchanges between rival states between 2000 and 2016. In categorizing those exchanges, they estimated 32% as disruptions, 54% as espionage, and 12% as degradation, or the most damaging types of attacks, meant to disable or fundamentally damage their targets. Most importantly, the study's authors concluded that most (68%) do not document a pattern of retaliation, concluding that most cyber operations do not beget attacks, nor do they deter them. They posit that a certain level of cyber operations is the norm and that while cyberspace to date has been a domain of political warfare and coercive diplomacy, cyber operations have not been escalatory or particularly effective in achieving decisive outcomes.¹⁶ "Incidents" or "attacks," regardless of their number, do not constitute a war—cyber or otherwise—in a true political, legal, operative, or factual sense.¹⁷ While many talk of a coming "Cyber Pearl Harbor," the authors sug-

¹⁵ Charter of the United Nations, effective 24 October 1945, Article 2(4).

¹⁶ Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford Scholarship Online, May 2018), <https://doi.org/10.1093/oso/9780190618094.001.0001>.

¹⁷ Mika Kerttunen and Eneken Tikk, "Strategically Normative. Norms and Principles in National Cybersecurity Strategies," *EU Cyber Direct*, April 13, 2019,

gest the domain is really littered with covert operations meant to manage escalation and deter future attacks. They counsel a defensive posture consisting of limited cyber operations aimed at restraining rivals and avoiding escalation instead of recent policy changes and strategy pronouncements by the Trump administration that suggests that offense is an effective and easy way to stop rival states from hacking America (a posture the authors note as a dangerous myth).

Some argue that cyber operations offer an effective means to diffuse and de-escalate, and rather than persistent action and preemptive strikes, America needs to use cyber operations to sow persistent deception and active defenses.

International Politics as a Tool for Managing Cyber Relations

A central component of President Obama's position was cyber deterrence and working towards international norms of behavior. His 2011 International Strategy for Cyberspace laid out three core principles: 1) ensuring fundamental freedoms such as freedom of expression; 2) privacy; and 3) the free flow of information. In 2015 Obama reached a deal with the Chinese to limit cyberattacks, with a subsequent reduction in their number. President Trump has taken a different position, sparking increased Sino-American tensions with trade policies and a US Cyber Command position¹⁸ calling for "persistent action to maintain cyber superiority." His position is one of active engagement and defending against outside networks. Do such aggressive stances and policies for authorizing preemptive offensive cyber strategies risk crossing a threshold and changing the rules of the game?

In May 2019, the NATO Secretary General told Russia and other potential foes that the Western military alliance was ready to use any and all possible means at its disposal to respond to cyberattacks. "For deterrence to have full effect, potential attackers must know we are not limited to respond in cyber space when we are attacked in cyber space," Stoltenberg said during a joint press appearance in London with UK Foreign Secretary Jeremy Hunt. "We can and will use the full range of capabilities at our disposal."¹⁹ Do such aggressive stances and policies for authorizing preemptive offensive cyber strategies risk crossing a threshold and changing the rules of the game?

https://eucyberdirect.eu/content_research/a-normative-analysis-of-national-cybersecurity-strategies/.

¹⁸ United States Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," June 14, 2018, www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

¹⁹ "NATO Warns Russia of 'Full Range' of Responses to Cyberattack," *Security Week*, May 23, 2019, <https://www.securityweek.com/nato-warns-russia-full-range-responses-cyberattack>.

Conclusions

A number of nation state-linked cyber threats have emerged over the last decade that have left nations feeling insecure, including surveillance/attacks on critical infrastructure, interference in internal affairs of other countries through Internet/social media-based propaganda, financial fraud, theft of intellectual property, and compromising national security. In reacting to these threats, nations are tightening their Internet borders. Unless countries feel secure, this tightening of Internet borders will continue and spread rapidly, and until the Internet is truly demilitarized, countries will not feel secure. In the absence of effective and verifiable norms, we should expect to see a continued tightening of Internet borders and increased surveillance of the Internet and social media. Countries will continue to build their cyber arsenals as a deterrent against other nations; this will include misinformation campaigns, destabilizing attacks, probing cyber defenses, and gathering intelligence. Without trust and mutual cooperation, it will be hard to build consensus on norms, and this trend will continue and could lead to the eventual complete fragmentation of the Internet; perhaps in a classic East-West divide, which is not a desirable state.

First, if we let this trend continue unmitigated, we will be retreating from much of the gains we have already realized and limit the opportunity to continue to reap rich rewards from our connectivity in terms of better health, education, economic stability, and better quality of life. We need to find a balance that allows for the free flow of information while protecting sensitive information, based on the societal and political expectations and security needs of each country. Second, we need to avoid to the degree possible the most catastrophic consequences of the misuse of the Internet, such as damaging health and energy infrastructure, proliferating child exploitation and trafficking of women, and national security dangers. This means creating red lines that everyone can rally around. Third, we need to ensure that cyber warfare does not inadvertently lead to kinetic warfare (including nuclear) through miscalculation or misattribution of the attacks. Finally, as we craft polity, we need to keep an eye on the importance of the Internet for society and understand the risks to the societal gains if we do not reach a global consensus on cyber warfare and limit the proliferation of cyber weapons.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

About the Author

Sanjay Goel is an Associate Professor in the Information Technology Management Department (School of Business) at the University at Albany, SUNY and Director of Research at the New York State Center for Information Forensics and Assurance at the University. Dr. Goel received his Ph.D. in Mechanical Engineering in 1999 from Rensselaer Polytechnic Institute. His current research interests include information security and privacy behavior, innovative education and pedagogy, security models, i.e., biological models, risk models, and security policies and cyberwarfare. He conducts research on forensics and cybercrime, and critical infrastructures, including privacy in smart grid data analytics; the impact of security and terrorism on financial markets; resilient transportation; and resilient service-oriented architectures. *E-mail*: goel@albany.edu.



Research Article

How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race

Sanjay Goel

New York State Center for Information Forensics and Assurance, University at Albany, 1400 Washington Avenue, Albany, NY 12222

<https://www.albany.edu/cifa/>

Abstract: Cyber warfare is a critical component of nation-states' military arsenals, and a cyber arms race has emerged in the absence of international agreements (norms and confidence-building measures) to limit the use of cyber warfare. One key impediment to building consensus on cyber norms and confidence-building measures is a lack of transparency in cyber weapons development and poor attribution of attack perpetrators. Recently, there has been an improvement in attribution capabilities based on better data collection and the profiling of known hackers and nation states by intelligence agencies, and this should give impetus to efforts to establish confidence-building measures and cyber norms. This article discusses the need for and challenges associated with attribution, recent advances that will lead to better attribution, and the collective responsibility of nation states in addressing these challenges. It suggests several initiatives to reduce chances of cyber conflict, as well as to prevent cyber conflicts from escalating, such as defining clear processes for attribution, creating neutral bodies for incident analysis, and limiting the scope of retaliation based on the confidence in attribution.

Keywords: cyber warfare, cyber arms race, attribution, confidence-building.

Introduction

The prevalence and risk of cyberattacks continue to rise in parallel with our increasing reliance on the Internet for systems of economic production, supply and distribution chains, finance, power, transportation, and other critical infrastruc-

tures. Cyber warfare is becoming the next serious threat to national security¹ that can impact not only life and property but also financial markets.² According to the Centre for Strategic and International Studies (CSIS), the total number of cyber-attacks against government agencies, defense and high-tech companies, or economic crimes with losses of over one million dollars rose from 21 in 2014 to 58 in 2017.³ This CSIS list, built on open-source data only, depicts a worrisome trend of rising cyberattacks attributed to state-sponsored groups acting against the political or economic interests of other states.

In testimony delivered to the US Armed Services Committee in January 2017, James Clapper, former US Director of National Intelligence, stated that more than 30 nations were developing offensive cyberattack capabilities as of late 2016. He further opined that “the proliferation of cyber capabilities coupled with new warfighting technologies will increase the incidence of standoff and remote operations, especially in the initial stages of conflict.”⁴ As policymakers warn of the dangers of cyber conflicts and exalt the virtues of cyber peace, most states consider cyberspace the fifth operational domain, with equal, or perhaps greater future importance to the traditional domains of land, sea, air, and space. State military and intelligence agencies continue to conduct cyber espionage and covert attacks on computer systems and networks in pursuit of strategic political or military objectives, both before and during conflicts. Yet, there is limited transparency on how states consider using their cyber capabilities, as only a few countries have publicly announced their cyber doctrines and underlying strategies. For example, McAfee, the global computer security software company, estimated in 2007 that over 120 countries were working on cyber commands,⁵ whereas Dévai listed 114 countries that, as of 2013, were developing civilian and military cyber capabilities, policies, doctrines and organizations at varying levels of maturity or focus.⁶ Considering that many of the officially declared ‘defensive’

¹ Richard A. Clarke and Robert K. Knake, *Cyberwar: The Next Threat to National Security and What to Do About It* (New York, NY: Harper Collins, 2010).

² Sanjay Goel and Hany A. Shawky, “Estimating the Market Impact of Security Breach Announcements on Firm Values,” *Information & Management* 46, no. 7 (October 2009): 404-410, <https://doi.org/10.1016/j.im.2009.06.005>.

³ Centre for Strategic and International Studies, “Significant Cyber Incidents Since 2006,” 2018, accessed June 20, 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/180425_Significant_Cyber_Events_List.pdf.

⁴ James R. Clapper, Marcel Lettre, and Michael S. Rogers, “Joint Statement for the Record to the Senate Armed Services Committee ‘Foreign Cyber Threats to the United States,’” January 5, 2017, accessed June 14, 2018, https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf.

⁵ Arie J. Schaap, “Cyber Warfare Operations: Development and Use Under International Law,” *Air Force Law Review* 64 (2009): 121-173.

⁶ Dóra Dévai, “Proliferation of Offensive Cyber Weapons. Strategic Implications and Non-Proliferation Assumptions,” *Academic and Applied Research in Military and Public Management Science (AARMS)* 15, no. 1 (2016): 61-73, <https://folyoiratok.uni-nke.hu/document/uni-nke-hu/aarms-2016-1-devai.original.pdf>.

cyber capabilities could easily be deployed in offensive cyber operations, as well as the fact that data assembled by cyber experts is often based on publicly available information only, it is not surprising that such estimations vary, and that the true state of cyber warfare preparedness and capabilities worldwide is difficult to ascertain. This high degree of uncertainty, when coupled with the low cost and easy acquisition of cyber weapons, ample and growing target selection, and multiplicity of types of attacks that may go unnoticed for a long time, contributes to a prevailing state of cyber insecurity in the international community. The problem is further exacerbated by the fact that there is no commonly accepted terminology of critical cyber terms (e.g., 'cyber' vs. 'information' security) among key cyber actors, which affects the ability of most likely strategic adversaries to establish common ground as a prerequisite for dialogue.

Cyber warfare is a broad term that refers to actions by nation-state actors (or other international organizations with *mala fide* intentions) to use hacking tools to achieve military objectives in another country. The tools for hacking are varied and can include malicious software, denial-of-service attacks, social engineering, fake news, and malicious insiders as well as tools for camouflaging identify of hackers or misdirecting attribution. The objectives could be tactical or strategic. The tactical objectives could be degrading the capability of an adversary both in the battlefield or in weapons development (e.g., Stuxnet) or espionage to collect intelligence. The strategic objectives could be the use of soft power such as propaganda to influence public opinion for regime change or altering the political outcomes of the election or hard power by leaving dormant malicious software in critical infrastructure to leverage during times of conflict.

The boundary between conventional and cyber war is blurring as conventional defensive and offensive capabilities increasingly use the Internet for command, control, communications, and intelligence, making information and communication infrastructures and networks both the targets and vehicles of military attacks. At the same time, the Internet has become the communications backbone required for the functioning of modern societies and economic systems. Therefore, the nature and means of the military defense of these systems also have to change and become more flexible to adapt to these emerging threats. Above all, the nascent cyber defense mechanism of any state must be able to provide the national political leadership with answers regarding a number of critical questions: What is the origin of a cyberattack; where did it come from? Who is responsible? What is the recommended course of action, or response?

Attribution

Attribution of cyberattacks is very important, especially to justify retaliatory actions against the perpetrators and prevent accidental retaliation against innocent targets. The entire domain of cyber norms and confidence-building measures is centered on visibility, i.e., being able to identify perpetrators of attacks and being able to ascertain adversarial strength. In the absence of such

verification, the suspicion remains, and nation states assume the worst and prepare themselves by building stronger and stronger arsenals to maintain strategic equilibrium.

Anonymity is often regarded as a key foundational principle of the Internet, driven by the need to shield the identity of the user and dissociate users' actions from their identity.⁷ Such anonymity ensures the ability to speak freely without fear of retribution, which can be beneficial in political commentaries, debating contentious issues, asking personal questions, researching competitors, and purchasing goods or services without revealing personal choices. Privacy advocates have gone to great lengths to protect the anonymity of users by providing services, such as remailers and encryption, that further camouflage users' identities and protect them from government surveillance. However, while beneficial in some contexts and circumstances, such anonymity also shields the perpetrators of crime and terrorism on the Internet.⁸ The cloak of anonymity protects and enables perpetrators of money laundering, extortion, espionage, and theft. Similarly, actors engaging in cyber warfare leverage anonymity on the Internet to conduct surveillance, probes, and attacks without drawing attention to their actions. There has to be a balance between anonymity and security to ensure people's right to privacy and security.⁹

Forensics and Attribution

Despite the inherent anonymity of the Internet, users leave traces of their activities along the way. These traces can provide valuable clues that can reveal the identity of the attackers and their possible motivations. The goal of digital forensics is to collect the traces, connect the dots, and make inferences about the incident, including identifying the perpetrators, determining the mechanism of operation, and cataloging the information compromised or altered. The tools, processes, and knowledge for digital forensics are freely available. Still, the anonymity of the Internet makes such analysis difficult, especially in the case of cyber warfare, where relevant information of the attack is hidden behind country firewalls and protected by the sponsors of the attack.

Digital forensics can strip away some of the Internet's anonymity and narrow down the field of perpetrators by piecing these clues together and creating a chain of evidence that can link the attacker to the incident.¹⁰ Such evidential

⁷ Barry M. Leiner et. al, "A Brief History of the Internet," *ACM SIGCOMM Computer Communication Review* 39, no. 5 (October 2009): 22-31, <https://doi.org/10.1145/1629607.1629613>.

⁸ Helen L. Armstrong and Patrick J. Forde, "Internet Anonymity Practices in Computer Crime," *Information Management and Computer Security* 11, no. 5 (2003): 209-215, <https://doi.org/10.1108/09685220310500117>.

⁹ Sanjay Goel, "Anonymity vs. Security: The Right Balance for the Smart Grid," *Communications of the Association for Information Systems* 36, Article 2 (January 2015): 23-32, <https://doi.org/10.17705/1CAIS.03602>.

¹⁰ Sanjay Goel, "Cyberwarfare: Connecting the Dots in Cyber Intelligence," *Communications of the ACM* 54, no. 8 (August 2011): 132-140, DOI: 10.1145/1978542.1978569.

chains may not constitute irrefutable evidence in a court of law. Still, when combined with additional information such as legal, political, intelligence, and policy considerations, the resulting assessment could allow policymakers to formulate a national response to cyberattacks. From a national security perspective, as Healey argued, knowing “who to blame” can be more important than “who did it?”¹¹ A proper response to this question provides national authorities with the ability to assess the situation during an evolving conflict and weigh possible responses from a range of economic, diplomatic, or other tools at their disposal. As a multi-dimensional issue that draws on all sources of information available, including technical forensics, human and signals intelligence, historical precedents, and geopolitics, attribution of attacks to a state actor in cyber warfare requires a genuinely national effort and the development of corresponding technical and non-technical capabilities. It is through these processes of data collection and sharing, and analysis and cooperation conducted at national and international levels, that digital forensics becomes instrumental in the operationalization and practical evolution of a robust confidence-building measure (CBM) regime.

The tools and techniques of cyberattacks are common to “cyber warfare,” “cyber terrorism” and “cyber activism.” Only by analyzing the actors, modes of operation, and motivations behind attacks, and their intended or manifested targets, can one differentiate between the three. In contrast to conventional warfare, it is very difficult to distinguish whether attacks on a website or the online theft of data are attributable to individuals in another state who are motivated by financial gain, political or religious ideology, or actions taken by that state’s intelligence agency or military (or their proxies). Since states may launch cyberattacks via proxies in other states, attribution difficulties are compounded, and present fundamental challenges during both conflict and peace times, when international cooperation and treaty compliance verification take hold.

Digital forensics involves gathering data logged in different devices, including computers, routers, electronic industrial control systems, and mobile devices,^{12,13,14} putting it on the same timeline and making inferences to determine the anatomy of the attack/intrusion. Several pieces of relevant information can be used for tracing the activities of a person or a device, including IP-addresses,

¹¹ Jason Healey, “Beyond Attribution: Seeking National Responsibility for Cyber Attacks,” *Atlantic Council*, January Issue Brief 2012, https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF.

¹² Rizwan Ahmed and Rajiv V. Dharaskar, “Mobile Forensics: An Overview, Tools, Future Trends and Challenges from Law Enforcement Perspective,” in *6th International Conference on E-Governance, ICEG, Emerging Technologies in E-Government, M-Government* (2008), 312-23.

¹³ Terrence V. Lillard, Clint P. Garrison, Craig A. Schiller, and James Steele, *Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data* (Syngress Publishing, 2010).

¹⁴ Michael G. Solomon, K. Rudolph, Ed Tittel, Neil Broom, and Diane Barrett, *Computer Forensics Jumpstart* (Indianapolis, IN: Wiley Publishing Inc., February 2011).

domain names, and time stamps.¹⁵ These individual entries in different log files can be time-correlated to create a chain of evidence and demonstrate activity emanating from a specific source.

An equally important dimension of digital forensics is the detection of intrusion and post-incident analysis, whereby investigators need to understand how an attack was launched, what was stolen, damaged or changed, and how to prevent the attack from occurring in the future.¹⁶ This involves analyzing the internal logs of actors involved in the cyberattack and piecing together evidence from multiple sources into a single timeline of events. The evidence can be collected from hard drives, RAM, USB drives, storage devices, and network appliances. The fundamental problem with such analysis is the sheer volume of the data. Also, to forensically examine data from the past, it needs to be stored. Data storage limitations, especially network devices that generate enormous amounts of data, also limit the possible time frame of analysis.¹⁷ Other useful forensic techniques include analysis of social networks, as well as text analysis from social media to identify cyber warfare activities, such as propaganda, terrorist recruitment, or information exchange. Some of this analysis is done by hand, but a majority of it is done using automated tools that can sift through large volumes of text to flag relevant data for human analysts. Linguistic tools used for text analysis have become much more sophisticated over the last decade, from simple word counting to separating parts of speech and gaining limited language understanding. These forensic tools can help address the problems of attribution and provide means of dealing with contentious issues related to attribution and deflection of responsibility.

Forensics practices are well established and tools are available to rapidly analyze data and draw inferences from it. The data for analyses can be collected from devices and networks within organizations and Internet Service Providers (ISPs). There are, however, fundamental issues with forensic analyses and data collections that cross international borders and reach outside of a nation-state's jurisdictional control. First, much of the data is stored in routers and devices that are with the ISPs, which are subject to local laws. The data can be in multiple sources on the network and needs to be acquired before analysis. If data is not collected shortly after the incident, it can be overwritten. Consequently, administrative delays in coordination across countries can undermine forensics efforts. Additionally, if a state is complicit in the launch of an attack, the veracity of the data itself can be in question. The data could have been doctored, tailored, or completely faked. Second, getting physical access to the perpetrator's computer

¹⁵ Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (Boston, MA: Academic Press, May 2011).

¹⁶ N.K. McCarthy, *The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk* (McGraw-Hill Osborne Media, August 2012).

¹⁷ José Camacho, "Visualizing Big Data with Compressed Score Plots: Approach and Research Challenges," *Chemometrics and Intelligent Laboratory Systems* 135 (July 2014): 110-125, <https://doi.org/10.1016/j.chemolab.2014.04.011>.

requires a level of cooperation among countries that may be possible in cases of crime, but strained or nonexistent during cyber warfare. Third, all data can be spoofed, i.e., a fake address of origin can be used in packets to conceal the real IP-address, making the problem of identification even more difficult. Finally, the use of anonymizing tools can camouflage the perpetrators further, making attribution complicated.

All of these challenges make technical attribution for international cyber incidents difficult, though not impossible. It is still possible and has dramatically improved over the last few years through sustained intelligence efforts. In addition to data collected directly from ISPs and organizations, data can be collected through the use of honey pots and prepositioned data taps across global networks. Intelligence agencies are continuously monitoring the activities of known actors (including nation states). They are building intelligence dossiers that can be coupled with knowledge gained from digital forensics to make more definitive attributions.

Knowledge of previous events, tools, and techniques of known actors can be used to trace the origins of attacks. There is no automated analysis process; rather, analysts painfully evaluate evidence and make probabilistic judgments for assigning attribution. There are different levels of attribution, with each level becoming more difficult to assign attribution or point of origin (nation-state, hacker group), specific device (computer used to launch an attack), and an individual responsible for launching the attack. It is even harder to accurately pinpoint the sponsor of an attack, in cases where the hacker/group is working as a proxy.

Discussion

There are limits to what digital forensics can accomplish. These tools will only work to the extent that there is a political will for international cooperation in data sharing and analysis. Important first steps would include the establishment of hotlines and the deployment at strategic locations of standard data collection devices that could not be tampered with. These could be foundational to support the forensic analysis of cyberattacks and international determination of instances of cyber warfare. An international body needs to be created and deployed in a neutral country to monitor and evaluate cyber conflicts, with observers present from warring nations. This body would be able to quickly request data access from different sources; lengthy procedures can delay and limit the collection of data, which can be ephemeral. This body will also have the technical expertise to analyze large volumes of data and determine attribution, as well as to confidentially handle intelligence without having to reveal its sources.

Digital forensics practices were developed to effectively piece together the evidence in criminal cases where: the data footprint is small; there is physical access to devices; and the perpetrators involved are relatively inexperienced with camouflaging techniques. This is very rarely the scenario when attacks are perpetrated by well-trained professional hackers. As a result, intelligence agen-

cies have already adapted and scaled forensics procedures for nation-state cyberattacks; a lot of these practices are not yet in the public domain. We will need to create standard forensics procedures (publicly available) for investigating cross border attacks in which camouflaging techniques have been deployed.

Additionally, digital forensics is constantly lagging behind the torrid pace of technological evolution, both in types of applications and devices, as well as in volumes of data.¹⁸ In the coming years, digital forensics will need to be able to contend with the extremely high volumes of data, as well as the sophisticated camouflaging techniques that are used in cyber warfare to become a credible factor in the attribution of cyber warfare activities. To be able to stay on course, we need to have an international forensics research institute for researching and updating forensics practices as information infrastructures evolve (e.g., connected vehicles, human-implantable devices, self-driving cars). We also need to train experts in each country on best practices (tools and techniques) in digital forensics so that they can conduct their investigations.

We must realize that attribution may not always be perfect due to purposeful misdirection or limitations of the analysis itself. This was illustrated by the attack on Sony Pictures Entertainment in November 2014. A hacker group calling itself the “Guardians of Peace” released confidential Sony data onto the Internet, including personal employee data, vast email and password files, internal documents and communications, unreleased copies of motion pictures, and much more. There are two conflicting theories of attribution: one suggests that the North Korean government was behind the attack, given the similarity of the malware used to that used in previous attacks by the North Koreans;¹⁹ the other, based on linguistics analysis, suggests that Russians conducted the attack.²⁰ There is no conclusive proof supporting either theory, only circumstantial evidence based on the conventional triad of means, motives, and opportunity. To address this, we must resort to a probabilistic approach and define standards of attributions based on the confidence levels of attribution and permissible retaliation to prevent the disproportionate response from escalating into a kinetic conflict.

The demilitarization of cyberspace or a moratorium on the development of cyber weapons is no longer a possibility. However, nation states must come together to find common ground in cyber warfare starting with confidence-building measures, norms of behavior, and the applicability of international laws to reduce the possibility of a major catastrophic incident. Formal information sharing (both at CERT and diplomatic levels) and establishing hotlines will help de-escalate future cyber incidents. There needs to be consensus building at the

¹⁸ Simson L. Garfinkel, “Digital Forensics Research: The Next 10 Years,” *Digital Investigation* 7, Supplement (August 2010): S64-S73, <https://doi.org/10.1016/j.diin.2010.05.009>.

¹⁹ Kim Zetter, “Sony Got Hacked Hard: What We Know and Don’t Know So Far,” *Wired*, March 12, 2014, <https://www.wired.com/2014/12/sony-hack-what-we-know>.

²⁰ Zetter, “Sony Got Hacked Hard.”

United Nations and other established international bodies such as the Office of Security and Cooperation (OSCE) to find ways of building consensus among nation states on preventing cyber conflicts and building confidence.

Conclusions

The Internet is a major economic and societal driver and instrument of knowledge dissemination with huge economic, political, and national security consequences. It is also a place for data theft, espionage, fake news, political influence, and propaganda, as has been evidenced in the Middle East, South Asia, and Europe. Nation-state attacks are constantly growing both in terms of frequency of attacks and sophistication. Such attacks undermine its influence as societal glue and diminish its influence on economic prosperity. There have been efforts to stem the escalation of cyber warfare; however, it has been very hard to build consensus among nation states on the mechanisms for de-escalation of cyber warfare. Lack of transparency in cyber weapon development and attribution of cyberattacks has been a critical barrier to the acceptance of confidence building measures. Improvement in data collection (intelligence) and forensic analytics capabilities has given us a much better cyber incident attribution capability. By building consensus among nation-states on protocols and procedures for attribution and clarifying the applicability of international law, we can start to build consensus on CBMs and norms and make the Internet safer and enable it to thrive. The paper suggests several initiatives to reduce the chances of cyber conflict as well as to prevent cyber conflicts from escalating, such as defining clear processes for attribution, creating neutral bodies for incident analysis, and limiting the scope of retaliation based on the confidence in attribution.

Disclaimer

The views expressed are solely those of the contributing author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

About the Author

See p. 86 of the current issue, <https://doi.org/10.11610/Connections.19.1.07>.

Connections: The Quarterly Journal **Submission and Style Guidelines**


Connections accepts manuscripts in the range of 2,000 to 5,000 words, written in a lucid style for a target audience of informed defense and security affairs practitioners and academics. All manuscripts should be submitted to the *Connections* editorial office electronically at PfPCpublications@pfp-consortium.org. They should feature the author's name, current institutional affiliation, and a provisional title at the top of the first page, and should include footnotes where necessary. Additionally, authors should provide a manuscript abstract and keywords.

Preferred themes for journal future editions include:

- Arctic Exploitation and Security
- Arms Control and European Rearmament
- Challenges and Opportunities in Intelligence Sharing
- Countering and Preventing Violent Extremism
- Cybersecurity
- Defense Institution Building
- Future Security Scenarios
- Hybrid Warfare
- Limitations of Naval Power
- Migration and Refugees
- NATO's Unstable Periphery
- Putin's Russia: A Threat to Peace or a Threat to Itself?
- Terrorism and Foreign Fighters
- Trends in Organized Crime

For questions on footnotes and references, please refer to the Chicago Manual of Style, at http://www.chicagomanualofstyle.org/tools_citationguide.html.

Unsolicited manuscripts are accepted on a rolling basis at the discretion of the PfPC Editorial Board.



Cyber Security and Defense is a highly rated topic not only for now, but for the future, too, not only for governments, but for industry, academia, and think tanks as well. This edition focusses on National Cyber Defense Policies and the Way Forward of Germany, Austria, the United Kingdom, Israel, as well as Switzerland. Additionally, it includes academic perspectives to complete the different views on Cyber.

**For all information regarding
CONNECTIONS, please contact:**

**Partnership for Peace - Consortium
Managing Editor
Gernackerstrasse 2
82467 Garmisch-Partenkirchen, Germany
Phone: +49 8821 750 2256
E-Mail: PfPCStratCom@marshallcenter.org**

**ISSN 1812-1098
e-ISSN 1812-2973**

