KONRAD ADENAUER STIFTUNG

Regional Programme
Australia and the Pacific

PERISCOPE

Occasional Analysis Paper Series, Vol. 2

Cyber Security in a Contested Age – Geopolitical Challenges and Opportunities for Australia and Germany

by Katja Theodorakis and Dr. Clint Arizmendi

June 2019

Impressum

Periscope:

'Periscope' is the occasional analytical paper series of the Konrad Adenauer Foundation's Regional Programme Australia and the Pacific. Just like the real-world sighting instrument, Periscope is meant to broaden our view – taking in perspectives from different angles. In this instance, it seeks to bring together perspectives from Germany, Europe and the Australia/Pacific region in order to augment our understanding of contemporary issues in the area of foreign and security policy as well as energy, economic and social policy matters.

Authors:

Katja Theodorakis and Dr. Clint Arizmendi

Publisher:

Konrad Adenauer Stiftung (Australia) Limited
Regional Programme Australia and the Pacific
11/3 Sydney Avenue
Barton, ACT 2600
Australia
Tel: +61 2 6154 9322
www.kas.de/australia

Design, Layout and Typeset:

Konrad Adenauer Stiftung (Australia) Limited e.V. / Corporate Design
implemented by MBE Manuka.

This analysis paper is a result of the **'1st Australia Germany 1.5 Track Cyber Security Dialogue'.** This Dialogue, titled **"Mapping the Field: The New Ecology of Cyber Security Challenges"**, comprised a delegation of German cyber security professionals; government representatives; Australian policy-makers; academic experts; and private sector representatives.

The attendees discussed current and emerging threats and opportunities in cyberspace to enhance multi-agency and partner coordination and cooperation. The Dialogue explored crucial aspects of contemporary cybersecurity issues: geopolitical implications of a shifting global order; international cyber norms; military cyber operations; and public-private partnerships. It was held under Chatham House Rule to allow for a frank and confidential exchange on these matters. This paper is not a direct summary of the proceedings but draws on and further develops some of the key themes that emerged during the Dialogue.

Ultimately, it will demonstrate that in order to effectively manage and mitigate within a cyber ecosystem, a combination of political leverage, diplomacy, dialogue and deterrence is required in order to safeguard State sovereignty.

Table of Contents

Authors

Katja Theodorakis

KATJA THEODORAKIS is Programme Manager for Foreign/Security Policy and Counter-Terrorism at the Konrad Adenauer Foundation's Regional Programme Australia and the Pacific in Canberra. Her portfolio includes topics such as the wider strategic relations in the Asia-Pacific, cyber security, European defence/security matters and the field of terrorism/extremism.

She is also a PhD researcher at the Australian National University (ANU), where she focuses on Jihadi ideology, radicalization and foreign fighters. In particular, her research is concerned with anti-Western ideology and its strategic use in propaganda. Katja has previously traveled and lived in the Middle East, where she was engaged in educational projects and NGO work in Syria. She publishes and presents at seminars and conferences on the topics of national security, jihadism and Middle East politics, and has appeared on national TV and radio for commentary. At ANU, Katja has also been involved in teaching courses on Middle East politics and Islam, the West and International Terrorism.

She holds a First-Class Honours degree in International Development from the Australian National University, was recipient of an Australian Government Research (PhD) Scholarship, and has been awarded the 2016 ANU Media and Outreach Award as Emerging Media Talent.

Dr. Clint Arizmendi

DR. CLINT ARIZMENDI has a background in education and sociology. He worked previously for the Australian Department of Defence in the Emerging Threats and Opportunities cell in the Directorate of Future Land Warfare and he later joined the New South Wales Police Force Intelligence Directorate at State Crime Command.

Clint has worked across a variety of portfolios in an inter-agency and investigative targeting environment, ranging from terrorism and organised crime, to malicious non-state cyber actors, mis / disinformation and propaganda analysis. Dr. Arizmendi's current research interest is the intersection between social media and public safety. He currently leads the Intelligence and Information Security efforts for a global safety and welfare response company based in Sydney.

External Reviewers

The authors would like to thank the two external reviewers for their time and thoughtful comments to improve this paper: **Rachael Falk**, CEO of the Australian Cooperative Cyber Security Research Centre, and **Isabel Skierka**, research analyst and consultant with the Digital Society Institute (DSI) at the European School for Management and Technology (ESMT) in Berlin.

Preface

1st Australian-German 1.5 Track Cyber Security Dialogue "Mapping the Field: The New Ecology of Cyber Security Challenges"

We are very pleased to publish this analysis paper as a result of the first Australian-German 1.5 Track Cyber Security Dialogue, held in Canberra in June 2018. The Dialogue was a joint undertaking between the Department of Security Studies and Criminology (SSC) at Macquarie University and the Regional Programme Australia and the Pacific of the Konrad Adenauer Foundation. It brought together policy makers, government officials, business leaders and academics from Australia and Germany. The goal was to discuss the most pressing cyber security challenges and identify areas for further bilateral cooperation in this area.

The recommendations of the high-level Australia Germany Advisory Group (AGAG) set out the intensification of strategic dialogue and cooperation as a clear goal for our two countries. The Konrad Adenauer Foundation, being mentioned in the AGAG's progress report, certainly tries to contribute to this via different platforms for knowledge exchange and discussion together with its Australian partners: the already well-established annual Europe-Australia Counter Terrorism Dialogue for example, its Energy Security Dialogue and now adding the dialogue on cyber security.

Macquarie University has put a major emphasis on cyber security-related research and teaching programs, including the establishment of the Optus Macquarie University Cyber Security Hub, a $10million joint investment with Optus to tackle real world cyber security challenges. For many years, SSC has taught undergraduate and postgraduate cyber security programs. The department has also been a proud partner of the Department of Foreign Affairs and Trade (DFAT) in the delivery of international cyber security engagement projects.

It is a fact that cross-border cyber threats are real, with major ramifications for national security. This means that we are facing manifold challenges emanating from the information and cyber domain. Cyberspace is an evolving ecosystem and threat landscape which has effects on the foreign policy of our countries and the global security architecture in general.

Fighting cyber-related financial fraud, cybercrime and security threats in the digital age requires new ways of thinking, new technologies, and a new digital ecosystem to tackle evolving risks. The questions at stake here are:

How do we to protect ourselves against cyber attacks on critical infrastructure?

How do we develop global cyber norms?

How can we contribute to the evolution of cyber security policies?

Ensuring cyber security has thus turned into a central challenge for governments, the private sector and society, both at the national as well as the international level. And only a concerted response across all those sectors can guarantee success. Indeed, too often cyber security challenges are still treated as a predominantly technical problem, requiring a technical solution. While the technological dimension is certainly important, arguably the political, regulatory and societal frameworks are equally, if not more, critical to address the multi-dimensional aspects of cyber security. For instance, in times of major power shifts in the international systems, increasing great power rivalry, the struggle to stem the erosion of Europe, efforts to develop and implement effective international 'rules of the road' are facing significant challenges. Both Australia and Germany have been driving forces in international cyber diplomacy but have to keep the momentum.

Our conference addressed crucial aspects of contemporary cyber security challenges, ranging from the geopolitical level and questions about the shifting global order and international cyber norms to military cyber operations, private sector/industry perspectives, as well as the challenges of building the cyber workforce of the future. We were honoured by the presence and support of the keynote speaker, Dr. Tobias Feakin, Australia's Ambassador for Cyber Affairs at the Department of Foreign Affairs and Trade, who delivered the official opening address and also contributed to the panel on 'tackling the international cyber norm crisis'.

The Dialogue succeeded in identifying common cyber security interests between our two nations. Indeed, in a more fragile and uncertain world, like-minded, medium-sized powers such as Australia and Germany need to work even closer together to create a workable international cyber security framework and learn from each other's 'best practice'. The discussions also vividly demonstrated the vast untapped potential for much deeper Australia-German cyber security cooperation. Cyberspace does not break down geographical distances when it comes to practical cooperation. Therefore, creating habits of regular bilateral cyber cooperation will be crucial and it is hoped the next iterations of the dialogue will assist in this endeavour.

Prof. Benjamin Schreer
Head, Department of Security Studies and Criminology, Macquarie University

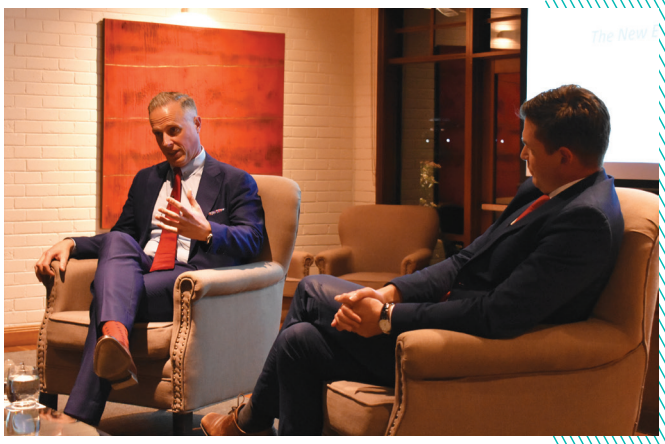
Dr. Beatrice Gorawantschy
Director Regional Programme Australia and the Pacific, Konrad Adenauer Stiftung

MACQUARIE University
SYDNEY·AUSTRALIA

KONRAD ADENAUER STIFTUNG

Panel discussion on cyber norms with the German and Australian Cyber Ambassadors Dr. Fitschen and Dr. Feakin (2nd and 3rd from left), chaired by Rachael Falk, CEO of the Australian Cooperative Cyber Security Research Centre (middle) and Fergus Hanson, Director of ASPI's International Cyber Policy Centre (far left)

Dr. Tobias Feakin, Australia's Ambassador for Cyber Affairs giving the keynote speech at the opening of the Dialogue



Dr. Tobias Feakin in conversation with Prof. Ben Schreer

Alastair MacGibbon, Australia's then National Cyber Security Advisor and Head of the Australian Cyber Security Centre (on the right), in the background, Lt-Gen. (ret'd) Kurt Herrmann, former Director of NATO Communication and Information Systems Services Agency

Introduction

Australia and Germany share similar challenges and approaches in this field. Questions at the forefront of policy-making debate query how governments can keep up with technology industry innovation that often out paces, if not drives, military adaptation.

How can deterrence and attribution be used effectively – from a national security perspective – against a backdrop of societies that seek to be increasingly anonymous and where privacy legislation, such as the GDPR (General Data Protection Regulation), has global implications for governments and the private sector alike? At the same time, the two countries' cyber security strategies also differ on a number of aspects; in this way, to compare and contrast approaches can be fruitful for gaining a deeper understanding of the problem-set and what can be done about it.

The Dialogue reinforced that the challenges of providing cyber security in a contested environment require holistic perspectives and highlights the need for more collaborative frameworks. As one participant observed, "the liberal order is in crisis – the dynamics of this are reflected in cyberspace, and particularly visible in discussions about cyber norms".

Based on a shared commitment to the rules-based order, Germany and Australia are well-positioned to continue to advance these discussions to build, and sustain, effective partnerships in this area.

The participants acknowledged it was critical to conceptualize this 'space' in a practical manner, especially given such conversations often fall victim to hyperbole. One participant called this tendency the "hollywoodization of cyber security", noting that the portrayal of the space often introduced exaggerated dangers and unrealistic capabilities. The challenge being that public perception – and misunderstanding – of cyber capabilities meant that expectations, and perceptions of the gravity of threat are often unrealistic. As a result, public confidence can wane quickly during an actual incident or protracted investigation. Public confidence is important because it is the foundation of political will. Likewise, other participants noted that framing cyber security predominantly in terms of threats – rather than opportunities – prevents recognition of its potential as an avenue for cooperation and combined exploitation in order to achieve mutually beneficial end states. This is something openly acknowledged by the German and Australian governments respectively, for example, in their collaborative efforts against ISIS. Using careful descriptions in the analysis of current and emerging threats and opportunities provides conceptualizations that resonate with non-practitioners as well.

Terms such as the 'global threat landscape', have been commonly applied, and – admittedly – criticized, in particular for their potential to overemphasize security challenges and 'normalize' perceived threats. As post – 9/11 notions of a 'global order under permanent threat' concur with the consequences of extensive technological expansion, we can witness a broadening and proliferation of security issues that reach into more and more areas of our lives.[1] Shifting the focus away from such a securitization lens is ultimately why the term 'ecology' or 'ecosystem'

Shifting the focus away from a securitization lens is why the term 'ecology' or 'ecosystem' was chosen, drawing attention to the symbiotic, yet fragile, nature of cyber security issues.

was chosen, drawing attention to the symbiotic, yet fragile, nature of cyber security issues. This metaphor is already employed extensively, having been used by the United States Department of Homeland Security and in the context of developing a more coherent strategic cyber security framework at the European Union level.[2]

At its most basic level, 'ecosystem' denotes the way organisms relate to each other and their surroundings, how they work together – or against – one another within a shared environment. The attendees viewed a cyber ecosystem as "a complex community of interacting devices, networks, people and organizations, and the environment of processes and technologies supporting these interactions".[3] Emphasis upon interconnectedness corresponds with the nature of cyber security as a field encompassing various subject areas: it is closely connected to traditional Information Technology approaches, including system administration, architecture, and penetration-testing, but also extends to the wider social science field.[4]

This means that what is supposed to be the remit of technical specialists as the technological capability has advanced and continues to be adopted and exploited by hobbyists, script-kiddies and amateurs who have the ability to maliciously affect an ecosystem with minimal effort. Moreover, what appear to be technical matters are interlinked with political, societal and ethical issues; how data and infrastructure protection is regulated also reflects competing interests, norms and approaches to security and economic interests. Taking the geostrategic climate into consideration, inherent in this metaphor is also the likelihood of imbalance, contagion and the inability to control all variables – hence the system's fragility and the need for resilience. However, as with all ecosystems, some will thrive; some will survive; and some will become extinct, meaning the ability to adapt rapidly is a key requirement.

Navigating the security challenges of the digital age, the most interconnected era in human history therefore needs to be premised on a nuanced understanding of its contesting forces. In this regard, it has become almost commonplace to assert that a whole-of-government, multi-stakeholder approach is required, both at the

national and international level. However, this often neglects to move beyond a mere recognition of the importance of such a coordinated, cooperative response. This is because it is at the same time challenging to coordinate a multi-stakeholder approach, especially in circumstances where there are competing and conflicting strategic interests. Hence, 'mapping the field' critically explored this ecosystem.

The question of what can be done to stem the negative effects of increasing cyber competition amongst nation-states – as part of an overall contested international environment – was a common thread throughout the various panels and discussions. One particular area identified as a priority was the question of effective deterrence and attribution beyond public 'naming and shaming' – which often seems to be an easily deniable, rhetorical device alone, with little consequences in the real world. It appears the effectiveness of deterrence (in the traditional sense) has to be questioned in the prevailing operating environment, with a dire need for capabilities that can address evolving security dynamics and vulnerabilities.

To this end, consolidated and concerted efforts are needed. As one participant put it:

> ***"Faced with growing risks and threats to security on the one hand and limited resources on the other hand, we witness an increased urgency for comprehensive cooperation between all parties and actors involved. Consolidated action of all relevant government resorts and close cooperation with international organizations involved are highly recommended. This needs to be extended to the area of comprehensive deterrence as well."***

These issues took even greater significance against the backdrop of apparent global attempts to interfere with elections using cyber capabilities that amplified misinformation and disinformation, potentially altering the ecosystems of democratic states.

Even when 'name and shame' was used by the entire US intelligence community to identify Russia as the lead actor, it had less effect than desired, given the perceived lack of US political will to address the issue. Furthermore, the sanctions imposed – presumably used to leverage economic power – were not as effective as possible; Russia managed to obtain World Cup and Olympic hosting; the concomitant critical financial boosts have the potential to offset the deleterious effects of such sanctions. As such, it is likely the lessons learned by adversaries with regard to the use of cyber capabilities to effect political and election outcomes will continue in the short-term. This is a threat not only to our collective sovereignty, but also to our socio-political ecosystem.

Although a comprehensive overview of contemporary cyber capabilities is not intended here, several distinct trends identified through the Dialogue will be addressed through contributions by some of the conference participants, each of whom has provided permission to publish their statements (some of them attributed, some under Chatham House Rule). These include:

- Attribution, deterrence and the problems associated with these concepts a shifting operating environment;
- The effect such trends have upon traditional methods of diplomacy, especially when the integrity and privacy of such engagements is no longer guaranteed;
- What defensive measures should look like. Are methods such as 'hacking back' effective and/ or productive?; What are our responsibilities and accountabilities, as democratic societies in choosing such measures?

Ultimately, the paper will demonstrate that in order to effectively manage and mitigate within a cyber ecosystem, a combination of political leverage, diplomacy, dialogue and deterrence is required in order to safeguard State sovereignty.

References

1 Jantunen, S & Hahtunen, A-M (2011), "American Perspectives on Cyber and Security: Coining the Linguistic Tradition", *Journal of Information Warfare,* Vol.10, No.3, pp.1-15; Dunn-Cavelty, M (2008), "Cyber Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate", *Journal of Information Technology & Politics,* Vol.4, No.1, pp.19-36; Dunn-Cavelty, M (2012), "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in Cyber-Security Discourse", *International Studies Review,* Vol.15, No.1, pp.105-122; Hansen, L & Niessenbaum, H (2009), "Digital Disaster, Cyber Security, and the Copenhagen School", *International Studies Quarterly,* Vol.53, No.4, pp.1155-1175.

2 Department of Homeland Security (2011), *"Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action"*, available under https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf; Lohrmann, D (2011), "What is a Healthy Cyber Eco System?", *Government Technology*, available under https://www.govtech.com/blogs/lohrmann-on-cyber security/What-is-a-healthy-061211.html; Papillo, L et al. (2018), "Strengthening the EU's Cyber Defence Capability: Report of a CEPS Task Force", *Centre for European Policy Studies,* available under https://www.ceps.eu/publications/strengthening-eu%E2%80%99s-cyber-defence-capabilities.

3 Ernst & Young (2014), "Achieving Resilience in the Cyber Ecosystem", *EY Insights on Governance, Risk and Compliance,* available under https://www.ey.com/Publication/vwLUAssets/cyber_ecosystem/$FILE/EY-Insights_on_GRC_Cyber_ecosystem.pdf, p.1.

4 Skierka, I and Schallbruch, M (2018), "Cyber security in Germany", *Springer Briefs on Cyber Security*, August 2018, p.4. https://doi.org/10.1007/978-3-319-90014-8

Defining / Situating 'Cyber': A Strategic Overview

One of the key challenges when engaging with the literature on 'cyber' activity is the absence of a universal definition. It is used as both a prefix and a noun, encompassing capabilities, activities, and threats. For the sake of this paper, we define cyber as a supporting or enabling apparatus to traditional methods and tools of national power and statecraft.

Accordingly, it has to be recognized that the word 'cyber', as for example used in 'cyber operations', 'cyber warfare' or 'cyber capabilities' has become ambiguous and amorphous, often treated as separate to traditional electronic warfare, signals, surveillance, and communications capability – a similar phenomenon that has occurred with 'drones'. Although considerable effort has been given to this process, the outcome has not always aligned with the intent, meaning there is significant disparity within and between operational definitions. The way a particular threat is framed within public and policy-making discourse has direct political and social consequences.[5] For instance, in the area of counter-terrorism, it has been argued that a pervasive 'securitization' discourse has, especially since 9/11, led to a routinization of previously exceptional security measures, thereby altering what is perceived as a 'normal' environment. Framings, definitions and language matter.

In the case of cyber security, competing and conflicting discourses have resulted in the development of differently weighted roles for states, non-state actors and individuals, as part of a securitization of the digital public sphere.[6] Hyperbole, such as warnings of an impending 'cyber Pearl Harbor' can therefore contribute to an overemphasis on national security, defence and a 'siloed' approach, neglecting to see it as a whole-of-society issue. When citizens view the cyber realm as a space to be defended solely by the government, it makes them more susceptible and vulnerable to malicious activity, ranging from scams and rorts, to influence activities. This creates a tension between education and resilience efforts and investment, and the operational offensive and defensive requirements of governments, especially when resources are limited.

In recognition of the constructed nature of security issues in general, it is important to avoid reductionist conceptualizations as well as definitional ambiguity. In response to the need for an integrated, comprehensive approach, in keeping with the current academic literature on cyber security, we identify four components as forming key parts of cyberspace, irrespective of the differing emphases attributed to them:

- Protection of personal and public data as well as intellectual property;
- Safeguarding economic interests;
- Protection of public and political infrastructure and
- Control of information and communication flows.[7]

This composition points to a conceptualization of cyber that encompasses political, strategic, and economic interests – extending to wider questions of power in international relations. Given its role in economic competition and politically driven conflict, it can be seen as a strategic enabler for statecraft, trade craft, conflict and warfare. In other words, coercive acts in cyberspace – across various avenues and

When trying to understand the current cyber environment, the ongoing centrality of geopolitical interests and contestations – alongside a new technological operating environment – demand a strategic perspective, geared towards sound attribution and deterrence mechanisms.

means – complement, rather than replace, traditional instruments of State power, a trend commencing several decades ago. For example, geopolitical competition over communications, black propaganda, 'active measures'[8] and 'information warfare' have been a feature of the international system since the beginning of the 20th century; however, cyberspace has enabled new ways of undermining democratic systems, both through the exploitation of digital mechanisms to spread disinformation as well as by compromising data integrity and confidentiality through IT-enabled attacks.[9]

In this way, cyber capabilities conveniently serve as an instrument of so-called grey zone capabilities (deniable, sub-escalatory actions by, often authoritarian, State-actors to advance their foreign policy needs).[10] When trying to understand the current cyber environment, the ongoing centrality of geopolitical interests and contestations – alongside a new technological operating environment – demand a strategic perspective, geared towards sound attribution and deterrence mechanisms. A clear perception of the dynamics of this contested space is vital, as highlighted by Dialogue participant Prof. Mario Voigt (see appendix for details and full contributions):

"Given the disparate actor and threat environment, where private and public spheres mingle, sovereignty and domains become blurry, democracies have to innovate their strategic thinking when it comes to cyber deterrence and think bigger. A more holistic approach is needed, which recognizes cyberspace as a strategic environment with distinct dynamics."

References

5 Buzan, B, Waever, O & de Wilde, J (1998), "*Security: A New Framework for Analysis*", Lynne Rienner, Boulder.

6 Dunn-Cavelty, M (2013), "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in Cyber-Security Discourse", *International Studies Review*, Vol.15, No.1, pp.105-122; Hansen, L & Niessenbaum, H (2009), "Digital Disaster, Cyber Security, and the Copenhagen School", *International Studies Quarterly*, Vol.53, No.4, pp.1155-1175.

7 Fichtner, L (2018), "What kind of cyber security? Theorising Cyber Security and Mapping Approaches", *Internet Policy Review*, Vol.7, No.2, pp.1-19.

8 We use this term in the traditional sense, referring to Russian activities commencing in the early 1900s, rather than the current way in which it has been appropriated and exploited by contemporary conspiracy theorists to drive fear within democratic societies, something that makes legitimate civilian education attempts much more difficult.

9 Tworek, H (2019), "Information Warfare is Here to Stay: States Have Always Fought for the Means of Communication", *Foreign Affairs*, April 25, 2019, https://www.foreignaffairs.com/articles/germany/2019-04-25/information-warfare-here-stay; Benett, L & Livingston, S (2018), "The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions", *European Journal of Communication*, Vol.33, No.2, pp.122-139.

10 Valeriano, B, Jensen, B & Maness, R (2018), *"Cyber Strategy: The Evolving Strategy of Power and Coercion"*, Oxford University Press, Oxford.

The Current and Future Operating Environment: Drivers and Trends

> ***"Cyberspace empowers states whose basic goals – sometimes grounded in a revolutionary domestic ideology, other times in the perverse visions of despots – are incompatible with the fundamental purpose of the international society: the preservation of a minimum measure of order and peace. More elementally, the technology also enables non-traditional players – proxy militias, political hacktivists, private corporations, extremist militant groups and even lone agents – who may seek to undermine the political order…"*** [11]

Disregarding hyperbolic warnings of impending 'cyberwars' or 'cyberstorms', it is clear that in this contested and hyper-connected age, as mentioned previously, cyberspace has provided distinct real-time disruptive opportunities for State- and non-state actors. Obstructionist activities, interference, attacks and information manipulation, for example, can all be undertaken at mass scale for relatively low investment, and often without requiring extensive skill. When combined with the challenges of attribution, which – in and of itself – can be resource-intensive, it directly challenges traditional diplomacy. This is because, despite their small-effort, low-cost attributes, such activities are often intended to have direct political consequences. Further complicating such efforts is the global threat of domestic infrastructure that is provided by foreign companies that covertly accept State sponsorship. As such, economic and information leverage is compromised before the political dialogue even commences.

These trends are illustrated by how revisionist powers such as Russia and China have worked in a targeted manner to gain a strategic advantage through cyberspace and the Information Environment (IE), often in conjunction with more traditional tools for geostrategic expansion and influence-building. Although this phenomenon is not necessarily 'new', Russia's election interference highlights how challenges to statehood and sovereignty continue seemingly unabated, something that blatantly challenges the rules-based order and for which governments have yet to develop effective deterrents. This is particularly problematic as nation-states like Russia have managed to exploit the current IE to seed and propagate political narratives that undermine other nation-state's political sovereignty at a very low cost. This is illustrated by Russian propaganda efforts during the German federal election in 2017 which actively sought to skew the public debate with the aim to weaken citizens' faith in the quality of their political system.[12] [13] Moreover, the manner in which Russia has used the 'Internet Research Agency' (IRA), a Kremlin-linked troll farm or 'election interference squad' to manipulate public opinion and discourse on social media platforms like Facebook, Twitter and Instagram is a salient manifestation of attempts at inducing polarization to undermine democracies.[14] In addition to the primary risk identified here, the secondary risk is that other actors mimic, or modify, the TTPs (Tactics, Techniques and Procedures) used to achieve their end state, being successful and undetected.

China is challenging sovereignty in a different manner, for instance through territorial claims to the self-proclaimed 'South China Sea' or the One Belt One Road (OBOR)'s infrastructure project aimed at widening the Chinese sphere of influence across the Eurasian subcontinent and across the Indian and Pacific Oceans. This entails the ability to

Disregarding hyperbolic warnings of impending 'cyberwars' or 'cyberstorms', in this contested and hyper-connected age, cyberspace has provided distinct real-time disruptive opportunities for State and non-state actors.

establish remote outposts, complemented by investment in foreign infrastructure, such as is evident in the Solomon Islands, Fiji, and Papua New Guinea. Part of the hard infrastructure building is a telecommunications component including supportive technology such as overland and submarine fibre optic cables as well as satellites. Complementing the geographic expansion, this so-called 'Digital Silk Road' extends to more comprehensive information and networking capabilities that enable the spread of communications and signals intelligence across a substantial part of the globe. It builds reliance. Considering the range of geopolitical interests tied up in the OBOR, there has been concern that this will lead to an increase in cyber espionage – highlighting an enmeshment of conventional and cyber tools of statecraft. More importantly, the projects are seen as part of a wider attempt to build a global communications network aimed at controlling the ICT sectors of participating countries (which for the most part are developing nations who lack adequate means to protect themselves from interference).[15] Even if they are not, the fact remains that the introduction of such significant communication infrastructure, without local training and development to manage it, builds an uncomfortable reliance upon the capability and the provider.

References

11 Kello, L (2017), *"The Virtual Weapon and International Order"*, Yale University Press: New Haven, p.2.

12 The so-called "Our Lisa" incident is emblematic of such overt measures: unfounded reports of a Russian-German teenage girl being abducted and raped by several 'Muslim' or 'Arab' men were widely shared by Kremlin-linked media outlets in Germany. The strategic dissemination of a false narrative at a time of heightened tensions over immigration further polarized public opinion and resulted in nation-wide political demonstrations, including in front of the Federal Chancellery. The end goal was to delegitimize democratic processes as a whole.

13 Saengerlaub, A (2017), "Fake News in the Shadow of the US and German Federal Elections", *Disinformation in the Digital Public Sphere Project, Stiftung Neue Verantwortung*, October 2017 (report in German only), https://www.stiftung-nv.de/en/project/disinformation-digital-public-sphere

14 Thompson, N and Lapowski, I (2018) "How Russian Trolls Used Meme Warfare to Divide America", *WIRED*, December 17, 2018 https://www.wired.com/story/russia-ira-propaganda-senate-report/

15 McLellan, C (2018, December 31),"Cyberwar Predictions for 2019: The stakes have been raised", *ZDNet*, available under https://www.zdnet.com/article/cyberwar-predictions-for-2019-the-stakes-have-been-raised/ Chipman, J (2019), "China's Long and Winding Digital Silk Road", *International Institute for Strategic Studies*, January 25, 2019, available under https://www.iiss.org/blogs/analysis/2019/01/china-digital-silk-road

As those methods above mature, and are used with greater efficiency, it is likely they will increase in frequency and severity, especially as people become increasingly globally connected. In the past decade, there have been increasing efforts – across States and the private sector – to identify the key trends that will shape their respective futures.[16] [17] [18] [19] Although the forecasters differ in their language, with some preferring 'meta-trends' to 'mega-trends', they are similar in their predictions. One consistent theme across the research is the notion that societies, globally, are increasingly technologically connected and reliant upon one another. Although global trade and commerce can benefit significantly from such connectivity, it carries risk, especially from a conflict perspective:

> ***"No country will have complete control over its communications infrastructure or control over the information that its citizens can access. Global telecommunications networks coupled with omnipresent communications technology will continue to empower non-state and semi-state actors. The effect will be disproportionate to their size and stature and allow the formation of supra-national organisations within the cyber domain. Large populations are also likely to be permanently connected to global networks, providing constant access to new 'real time' information. Access to social media, such as Facebook and Twitter, is widespread and accessible to both friend and foe, potentially allowing any individual to influence political outcomes, transform perceptions of events, and create positive or negative responses. This may dramatically affect the future use of military force." [20]***

Given the globe has surpassed 4 billion internet users,[21] and North Americans, Europeans and Australians are all expected to have multiple networked devices,[22] it is clear that connectivity's upward trend continues. With regard to vulnerabilities, to have numerous devices connected to multiple networks is a potential force multiplier for malicious activity, especially as it significantly increases the attack surfaces. Whether this means an increase in viruses, the spread of misinformation or disinformation, or increased social engineering opportunities remains to be seen. However, what has become evident is that opportunities for network and system exploitation have increased, as have the number of State and non-state actors willing to exploit them. According to the US National Security Council's 's Senior Technical Director, we are now in a situation where non-state hackers have reached similar to equal levels of sophistication as nation-states in terms of hacking capabilities for DoS attacks compromising privacy and data leaks. [23]

This is a particularly concerning trend – and a primary challenge for diplomacy – as everyday, *commercial off the shelf items* become easy targets – or tools – for disruptive cyber activity due to weak or ineffective protection mechanisms. Whether it be through the 'Internet of Things' (IoT), including 'Smart Home' devices such as Google Home or Amazon's Alexa,[24] or smart watches, even seemingly benign levels of malicious cyber activities can be problematic for governments due to their unpredictable effects. Even when they are low-threshold and the immediate perpetrators are criminals, they still require diplomatic engagement because of their effect on citizens; this is especially the case when the intrusion into digital privacy extends to essential nation-wide services, ultimately compromising technological sovereignty and national security. A salient example is the Mirai botnet, used for an IoT Distributed Denial of Service Attack that temporarily brought down the internet across the US and disrupted services in Europe in 2016.[25]

Consequently, hyper-connectivity has resulted in an increase of the number of stakeholders that are capable of driving geopolitical developments, with little guarantee of alignment of values or strategic endstates.[26] This means the diffusion of information technology has enabled not only higher effectiveness of communication, faster speed, and wider breadth of data exchanges, but also lowered entry thresholds and 'buy-in'. Hyper-connectivity has allowed traditionally less powerful States and non-state actors to access and develop capabilities previously restricted to more advanced powers with greater resources, whether through access to markets and products, or through IP theft. This trend may be an uncomfortable leveler of the playing field.

References

16 See PwC (2019), *"Megatrends"*, available under https://www.pwc.co.uk/issues/megatrends.html

17 See CSIRO (2019), *"Our Future World: Global Megatrends report"*, available under https://www.csiro.au/en/Do-business/Futures/Reports/Our-Future-World

18 See Office of the Director of National Intelligence (2017), *"Global Trends: Paradox of Progress"*, United States National Security Council, available under https://www.dni.gov/index.php/global-trends-home

19 See Australian Army (2014), *"Future Land Warfare Report"*, Commonwealth of Australia, available under https://www.army.gov.au/sites/g/files/net1846/f/flwr_web_b5_final.pdf

20 Australian Army (2014), *"Future Land Warfare Report"*, Commonwealth of Australia, available under https://www.army.gov.au/sites/g/files/net1846/f/flwr_web_b5_final.pdf, pp.11

21 Kemp, S (2018), "Digital in 2018: World's Internet Users Pass the 4 Billion Mark", *We Are Social*, available under https://wearesocial.com/blog/2018/01/global-digital-report-2018

22 CISCO (2019), *"Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper"*, available under https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html

23 Vavra, S (2019), "National Security Council Cyber Chief: Criminals are Closing the Gap with Nation-State Hackers", *Cyberscoop*, April 25, 2019, https://www.cyberscoop.com/cybercriminals-nation-state-tools-grant-schneider/

24 European Commission (2017), "Hyperconnectivity & IoT", available under https://ec.europa.eu/knowledge4policy/foresight/topic/accelerating-technological-change-hyperconnectivity/hyperconnectivity-iot-digitalisation_en

25 See for example Stephens, T (2018), " Internet of Things: When Objects Threaten National Security", *The Conversation*, May 29, 2018 https://theconversation.com/internet-of-things-when-objects-threaten-national-security-96962

26 Bremmer, I (2019, January 8), "The Geopolitics of 2069 Are More Chaotic Than You Can Imagine", *Medium*, available under https://medium.com/s/2069/the-geopolitics-of-2069-are-crazier-than-you-can-imagine-a7d9d4392abf

Examining the Tool-Kit: The Utility of Deterrence, Attribution and the International-Norms-Framework

It follows that in this strategic environment, the common rules of deterrence don't apply. It has been noted by security scholars that there is a qualitative difference to nuclear deterrence as it worked in a bipolar world order where traditional signaling to the adversary was based on a relative balance of power. In particular, it is argued that an effective deterrence framework for the cyber realm requires a strengthening of defensive and offensive networks that requires the development of new capabilities so that real costs can be imposed.[27]

On deterrence, the following participants commented:

> ***"The credible demonstration of cyber deterrence capabilities appears to be quite a difficult task. Any disclosure of active or passive cyber defence capabilities could rapidly devalue these capabilities, because opponents will be permitted to quickly adapt their own offensive or defensive capabilities. However, as cyber capabilities and operations in the cyber and information domain need to be fully integrated in a comprehensive approach on preventive security provisions and defence strategies."*** Lt.-Gen. (ret'd) Klaus Herrmann, President of the Clausewitz Society

Mario Voigt, Professor of Digital Transformation at the Quadriga University in Berlin, explains the deterrence conundrum in cyberspace as follows:

> ***"Deterrence seeks at its core to preserve the 'status quo' by persuading adversaries not to do something. However, in a cyber age insidious state or non-state actors continue to leverage all facets of the cyberspace in dynamic, proactive fashion to achieve a fundamental shift in global power toward their advantage.***

> ***Research scholars appear divided on if the deterrence still applies in cyberspace. Joseph Nye recently specified four key mechanisms for cyber deterrence: denial, punishment, entanglement, and norms. Others do not see in deterrence a credible strategy anymore, because cyber is an entirely new strategic environment, one which has important distinctions from the traditional domains of land, sea, air, and space. But how can democracies operate in such environment and respond accordingly?"***

Asking what democracies – not just States – can do is an important angle from which to tackle this issue as it connects to wider normative issues and institutional mechanisms in the rules-based order.

Within the current international framework, States seem free to propagate 'norms' and legal interpretations that align with their strategic and ideological interests. Arguably, in the absence of effective enforcement mechanisms a universal 'law' or 'cyber rulebook' has not served as a deterrent for such behavior. The Tallinn Manual 2.0 – despite seeking to offer a comprehensive regulatory scheme – seems to have only highlighted the normative ambiguity and lack of credible international enforcement mechanisms.[28] Similarly, in 2017 the fifth, and so far last, of the UN Group of Governmental

Whilst discussions on norms are important, current State behavior significantly undermines their likelihood and utility.

Experts (UN GGE) were unable to agree on a consensus report that would have brought additional clarity how international law regulates cyberspace.[29] As highlighted by researchers from The Digital Society Institute in Berlin, progress at the global level has been halting as of 2017 when the UN GGE failed to come to an agreement. In this way, UN negotiations, multilateral and multi-stakeholder processes have not resulted in a binding set of rules or tangible policy results.[30] Moreover, Russia has reportedly been attempting to establish an 'alternative' channel for UN discussions on cyber norms outside of the GGE, which, intended as a counter-weight to the official process, has the potential to significantly delay – or derail – any consensus on international cyber norms.[31]

This shows that – whilst discussions on norms are important – current State behavior significantly undermines their likelihood and utility. Both Germany and Australia have experienced cyber attacks on their Parliaments which exposed their vulnerabilities to potential exploitation or interference in their democratic processes by adversarial State actors. Following the 2016 Russian interference in the US elections, and the 2015 Bundestag hack, there has been growing concern about the safeguarding of liberal democratic institutions. This is primarily because of the concerns associated with direct foreign influence in domestic political affairs, but also because meddling with such processes would – at its logical conclusion – enable a malicious State to accumulate such significant power and influence that it would render itself uncontrollable. While the impact of such incidents varied in severity from country to country, they nevertheless serve as reminders of the reality that this trend continues without actors being deterred, as well as the possible consequences in terms of harming democratic processes.

As Australia was preparing for its 2019 federal election, revelations that its major political parties had been hacked in an attack on the Parliament's computer network in February 2019 have given rise to fundamental debates about the risks of interference in democratic processes. Arguably, as Major General Marcus Thompson, Head of Information Warfare at the Australian Department of Defence, noted, it is feared that the agencies and organizations responsible for fighting and countering such efforts are under-resourced.[32] Moreover, it is assessed that the upcoming European Union elections are at significant risk of disruption by disinformation and IT-enabled cyber attacks – with a dire need for better data infrastructure

protection.[33] This is particularly concerning given that EU investigators and academic experts have warned that the observed disinformation campaigns bear the same hallmarks as previous Russian attacks, meaning that "despite indictments, expulsions and recriminations, Russia remains undeterred in its campaign to widen political divisions and weaken Western institutions." [34]

Attribution is a key issue in the context of such attacks, as seen when the US intelligence community publicly outlined Russia's involvement. However, this is not a straightforward issue as Dr. Thomas Fitschen elaborated:

> ***"What is often simply called 'attribution' of a malicious cyber operation – or even simpler 'name and shame' – is actually a fairly complicated, multi-layered process. It is not a mathematical operation, but the assessment of a situation with lots of variables and few certainties. At the initial level attribution requires a process (often called 'cyber forensics') that tries to establish the technical (IT-)facts. What is it that we see going on in our systems? Where does the malicious code come from, and can we identify the way it got here? Can we find an IP address, a server, the PC that was used? And what exactly is the 'damage', if any? That is often terribly difficult to ascertain, but not always outright impossible."***

Responding to the attack on its parliamentary computer network, the Australian Government publicly declared it had identified a 'sophisticated State actor' yet without directly attributing the attack to a particular country.[35] Traditionally, Australia has only made official attribution statements as part of the Five Eyes alliance, with other states supporting its claims. In response to the official statement by the Australian Prime Minister and the involved security agencies, analysts highlighted the need to better define this act, urging for analytical clarity in determining its significance. In particular, the question of what consequences should be drawn if it were officially classified as an act of election interference? [36]

David Sanger, national security correspondent for the New York Times and author of *'The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age'* addressed this issue during a recent visit to Australia. He recommended that Australia should publish any evidence it may have on who is behind the attack, supported by concerted international action to send a strong signal:

> ***"I think it's in their [Australia's] strong interest to publish that data, publish the indicators, get as close as they can to indicating who it is who launched it, if they've got that data, because they want to show the Chinese Ministry of State Security that this is not a free ball, and that there will be consequences... Australia is really good at this. I mean, its signals intelligence (SIGINT) operation is known as one of the best in the world. So would it be nice if you bring in GCHQ or the NSA or somebody else to do an independent look, and come and announce their conclusion?" [37]***

Yet, it needs to be kept in mind that this is a complex issue.

As one Dialogue participant aptly put it, "there might be strategic reasons why a State *may choose not to attribute*: an absence of public attribution does not mean an absence of capability in *being able to attribute*."

Additionally, Australia's cyber security strategy boosts significant investments in offensive capabilities in the military space. To illustrate, the conceptual framework for Australian Defense Force (ADF) cyberspace operations emphasizes self-defense, passive defense, active defense before moving to offense.[38] The 2017 Cyber Engagement strategy however contains an open admission of their existence and Australia's willingness to use them, with a recent disclosure by the Australian Signals Directorate (ASD) releasing details of offensive operations against IS.[39] This was part of an unprecedented move to 'come out of the shadows', as the ASD Director-General put it.[40] This act may be considered part of a broader deterrence effort.

This is where the Australian approach significantly differs from Germany. In keeping with its traditionally pacifist post-war foreign and security policy stance, Germany has been reluctant to engage in offensive activities. In the case of the 2015 Bundestag attack, the head of the BND (the German foreign intelligence service) was cautious to directly attribute the attack to Russia publicly; the director of the domestic intelligence service, however, was more forthright, connecting the hack to the strategic context of Russian interference in Germany's democratic processes by a foreign power. Germany also set up a new military cyber command with a mandate to develop offensive capabilities to function as a deterrent and changes to the legal framework to authorize hack-backs have been discussed. Nevertheless, the German Cyber security strategy from 2016 is still mainly preventative, focused on IT security; this is complemented by the Bundeswehr's (Germany's Federal Armed Forces) 'active defense measures' – these appear to be solely used to protect its own capabilities however, which is partly to do with the legal limitations set out in Germany's constitution.[41] [42] Moreover, as of 2018, the cyber security architecture in Germany has been described as "characterized by competence wrangling" between security agencies as well as between the state and industry whose cooperation and coordinated efforts are in need of improvement.[43]

This has resulted in an ongoing debate in Germany about active cyber defense, the possible utility and normative implications of hack-backs as an efficient tool as well as the need to extend beyond preventative measures alone to ensure diplomatic and democratic stability.

With regard to possible options and their limitations, the utility of hack back, as an offensive capability and effective deterrent, has been discussed. The practice, being illegal in countries like the US, Germany and Australia, is nevertheless subject to industry rumors and also political debate. As purportedly demonstrated by the controversial 2013 Mandiant report, hacking groups linked to nation-states pose a new geopolitical risk, but are often mainly tracked by private firms.

Whilst the report has been scrutinized over a number of issues – including its independence – it has raised ongoing questions on whether legislation should be introduced to allow hack-back for private companies.[44] The commonly cited concerns with hack back are difficulties in attribution, risking mal-attribution as well as the danger of 'digital vigilantism' and provoking retribution- all of which would escalate malicious activity. This way, States rely on diplomatic tools such as MoUs, attribution, 'naming and shaming' as well as straightforward criminal prosecution for private individuals and entities.

These attacks and subsequent responses clearly show how this environment of openness and connectivity is exploited, and the need for sound defense and deterrence mechanisms. Yet, what these incidents also demonstrate is that no visible costs have been imposed, for example, in the form of sanctions. To illustrate, on the attribution problem and the feasibility of deterrence, it has been noted that:

> ***"[c]heap talk – unenforceable indictments, minor sanctions, and 'name and shame' tactics – has not prevented historical attacks, and policymakers perceive more significant punishment to be too costly, too risky, or too escalatory to enforce."*** [45]

Additionally, comparing different countries' cyber security strategies shows that definitions of defence and offence vary greatly, with no common vocabulary to draw on as the basis for concerted, coordinated efforts. Deterrence by norms is clearly not enough, declaratory rhetoric alone does not make for good policy that can respond effectively to the challenges present – in harnessing capabilities, exploiting opportunities, and overcoming vulnerabilities.

Prof. Mario Voigt sketches this unique situation as follows:

> ***"Old habits die hard, and outdated thinking harder still. Deterrence in a cyber age means an operational environment and strategy of constant action, permanent contact and ongoing contests with adversaries. Hence, the global digital ecosystem demands not just a pure military response. Recent attacks like in Germany proved a more holistic, even international, approach is needed including a range of political, social, economic, technological and legal responses. Security is achieved through imposed norms, clear expectations of state behavior, cooperation with non-state-actors, on an international level, but also a cyber initiative mindset. Deterrence, yes but different."***

This calls attention to what we can do about these challenges and dilemmas concomitant in the current ecosystem. Referring to an initiative-focused mindset puts the onus on proactive, rather than reactive, action. Despite the aforementioned shortcomings, both Germany and Australia are respectively in an opportune position to make progress in the area of cyber security and cyber policy development over the coming years.

References

27 Nye, J S (2017), "Deterrence and Dissuasion in Cyberspace", *International Security*, Vol.41, No.3, pp.44-71.Painter, C (2018), "Deterrence in Cyberspace: Spare the Costs, Spoil the Bad Actor – Deterrence in Cyberspace Requires Real Consequences", *Australian Strategic Policy Institute*, June 1, 2018, https://www.aspi.org.au/report/deterrence-cyberspace

28 Efrony, D & Shany, Y (2018), "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice", *American Journal of International Law*, Vol.112, No.4, pp.583-657

References

29 Henriksen, A (2019), "The end of the road for the UN GGE process: The future regulation of cyberspace", *Journal of Cyber security*, Vol.5, No.1, pp.1-9

30 Schallbruch, M, Gaycken, S & Skierka, I (2018), "Cyber security 2018-2020: Proposals for action for the CDU/CSU and SPD", *DSI Industrial & Policy Recommendation Series*, Vol.1, available under https://www.esmt.org/pub/cyber security-2018-2020-proposals-action-cducsu-and-spd

31 Vavra, S (2019), "DSN Hacks are Attacks on Critical Infrastructure, Senior US Diplomat Says", *Cyberscoop*, April 24, 2019, https://www.cyberscoop.com/dns-hacks-robert-strayer-united-nations/

32 Borys, S (2019), "Senior Defense Figure Raises Concerns About Future Cyber Attacks - and the Scenario Costing Him Sleep", *ABC News*, February 19, 2019 https://www.abc.net.au/news/2019-02-19/australian-army-under-cyber-attack-major-general-marcus-thompson/10822966

33 Bendiek, A & Schulze, M (2019), "Disinformation and Elections to the European Parliament", *German Institute for International and Security Affairs (SWP)*, SWP Comment 2019/ C16, March 2019, https://www.swp-berlin.org/en/publication/disinformation-and-elections-to-the-european-parliament/

34 Apuzzo, M and Satarino, A (2019), "Russia is Targeting Europe's Elections. So are far-Right Copycats", *The New York Times*, May 12, 2019,

35 Tillett, A (2019), "Chinese Spies Suspected in Cyber Attack on Major Parties", *Australian Financial Review*, February 18 2019, https://www.afr.com/news/politics/cyber-attack-on-major-parties-computer-systems-scott-morrison-reveals-20190218-h1bdzm

36 Cave, D & Uren, T (2019), "Espionage or interference? The attack on Australia's parliament and political parties", *The Strategist*, available under https://www.aspistrategist.org.au/espionage-or-interference-the-attack-on-australias-parliament-and-political-parties/; Stilgherrian (2019, February 26), "Australia should name parliament cyber attackers", *ZDNet*, available under https://www.zdnet.com/article/australia-should-name-parliament-cyber-attackers/; Sear, T (2019), "A state actor has targeted Australian political parties – but that shouldn't surprise us", *The Conversation*, available under https://theconversation.com/a-state-actor-has-targeted-australian-political-parties-but-that-shouldnt-surprise-us-111997

37 Quoted in ASPI (2019), "Cyber Frontier Wars: What's Next: In-conversation with The New York Times' David E. Sanger", available under https://www.facebook.com/ASPI.org/videos/245467296358957/

38 MacLean, A (2019, February 18), "Australia has a challenge of scaling defense capabilities for larger cyber attacks", *ZDNet*, available under https://www.zdnet.com/article/australia-has-challenge-of-scaling-defence-capabilities-for-a-large-scale-cyber-attack/.

39 Grigg, A (2019), "Australia Claims World-First in Cyber War", *Australian Financial Review*, March 27, 2019, https://www.afr.com/technology/technology-companies/australia-claims-world-first-in-cyber-war-20190326-p517q6; Burgess, M (2018), "Mike Burgess, ASD Director-General Speech to the Lowy Institute", March 27, 2019, https://www.asd.gov.au/speeches/20190327-lowy-institute-offensive-cyber-operations.htm

40 At the same time, he highlighted that "coming out of the shadows doesn't mean that we will be able to talk about the detail of our operations. Some things will need to remain classified out of necessity." https://asd.gov.au/speeches/20181029-aspi-national-security-dinner.htm

41 Herpig, S (2017), "Cyber Operations: Defending Political IT Infrastructures", *Stiftung Neue Verantwortung*, Policy Brief, available under https://www.stiftung-nv.de/sites/default/files/tcf-defending_political_It-infrastructures-problem_analysis.pdf

42 As opposed to Australia, where the main responsibility lies with the Australian Signals Directorate (ASD) – a statutory agency within the defence portfolio - in Germany the central cyber security agency is the BSI – the Federal Ministry for Information Security. It is an entirely civilian agency that has no police or intelligence powers and is only permitted to conduct active operations outside federal networks in cooperation with the public prosecutors' offices and police forces. See Skierka, I and Schallbruch, M (2018), "Cyber security in Germany", *Springer Briefs in Cyber security*, August 2018, DOI: https://doi.org/10.1007/978-3-319-90014-8

43 Schallbruch, M, Gaycken, S & Skierka, I (2018), "Cyber security 2018-2020: Proposals for action for the CDU/CSU and SPD", *DSI Industrial & Policy Recommendation Series*, Vol.1, available under https://www.esmt.org/pub/cyber security-2018-2020-proposals-action-cducsu-and-spd, pp.1

44 C Bing (2018), "FireEye Denies Hackback Claim Detailed in New Book", *CyberScoop*, June 25 2018, https://www.cyberscoop.com/fireeye-hack-back-david-sanger-book/ ; S Vavra (2019), "Congress is Taking Another Stab at Hack Back Legislation", June 13 2019, Cyberscoop, https://www.cyberscoop.com/hack-back-bill-tom-graves-offensive-cybersecurity/

45 Lindsay, J R (2015), "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack", *Journal of Cyber Security*, Vol.1, No.1, pp.54

What Can Be Done: Recommendations

The basis of Australia and Germany's foreign and defense/security policy is a commitment to the rules-based order. Within this framework, there is – despite obstacles, such as state-behavior contravening international norms – scope for action that can build on this common foundation.

As partners, Germany and Australia both adhere to legal and ethical guidelines when countering adversary cyber action that does not follow such rules – an obligation which should be seen as a source of strength rather than a constraint. Yet, participants, throughout the Dialogue and in their contributions here, have repeatedly asked 'what can democracies do'? The collective agreement that cyber exploitation is now more pervasive, accessible, and dangerous than before requires both enhanced dialogue and diplomacy, but also effective deterrence mechanisms applied by numerous stakeholders simultaneously. Otherwise, there is potential for a loss of sovereignty.

One key theme running through this paper has been the context from which the current challenges have arisen, in particular the complexities, dilemmas and vulnerabilities emanating from a hyper-connected operating environment with more diffuse actors and blurred boundaries.

Connectivity without values creates new spaces where power can be abused by actors that don't adhere to the tenets of the rules-based-order. Power that is not only obtained under false means, but also sustained by a system with loopholes creates a cyber ecosystem in disequilibrium.

Yet this quandary is also where we need to look for opportunities. Collaborative efforts to safeguard information and infrastructure can decrease the influence of foreign malicious actors, whether State or non-state. Both Germany and Australia advocate through their cyber security strategies whole-of-government solutions with a strong focus on diplomacy. This often entails integrating the elements of foreign and defense policy based on liberal values, comprehensive domestic legislation and strong collaboration with industry and the private sector. In particular the issues of Critical Infrastructure Protection and Threat Information Exchange would be suitable areas for increased dialogue and cooperation, also including IT Industry partners. In this regard, it is important to note that in the EU, as well as in Germany, the protection of critical infrastructure is far more regulated than in Australia – meaning that it could serve as an instructive topic for further comparative work.

Arguably, the best weapon is an integrated approach domestically and globally – this includes a better coordination of national cyber defenses and an internationally cohesive stance against State-sponsored cyber actions. Learning from each other to close capability gaps can be a way forward in this environment. Moreover, what the first dialogue – the fact that people took the time to sit, think and talk together frankly – highlighted is a commitment to further cooperation and official engagement, ensuring that the alliance is strong. The global friction – and the unpredictability of certain governments – means that such alliances are going to become increasingly important. In times of risk and volatility, strong relationships with like-minded partners matter more than ever to deter adversaries.

Based on the arguments presented in this paper, it can therefore be concluded that to effectively manage this cyber ecosystem, **a combination of political leverage, diplomacy, dialogue and deterrence should be employed to safeguard State sovereignty.**

The following contributions from participants illustrate this further:

Dr. Fitschen:

"As to the possible means for a reaction, international law provides a vast array of countermeasures, to be utilized in a calibrated, proportionate and effective way. The decision to go down that road, ideally together with partners and allies who are equally affected, is in any case the sovereign prerogative of the government. It is an intrinsically political act. In view of the legal and political difficulties involved, Germany and Australia have for many years engaged in activities at the UN to advance a common understanding of the international law that applies to such cases, and have advocated for clearer norms of responsible state behavior in cyberspace, confidence building measures and capacity building."

Lt-Gen. (ret'd) Herrmann:

"Particularly, the focus must be on rapid detection and analysis of abilities, intentions and concrete effects of potential opponents. Thus, joint intelligence, surveillance and reconnaissance as well as massively improved on-line forensic capabilities are considered to be priority tasks of cyber defence and predominantly of comprehensive deterrence."

Prof. Voigt:

"Democracies need agile policies which allow for offensive and defensive measures as well as anticipating and integrating the technological change coming. Defending forward with persistence and active engagement will guide a deterrence by retaliation, which holds adversaries accountable and impacts their risk calculus. Moreover, a comprehensive approach of cyber security emphasizing resilience will include private and public actors in unique way. In most democracies the private sector owns infrastructure and data, has the biggest cross-national interdependence and is conceptional better equipped for the cyber age. Building resilience and focusing on the cyber ecosystem is part of a deterrence by denial, which includes capacity building, shared incident reporting and response, expanding quantity and quality of digitally literate people, technological research and development. Hence, collaboration has to be expanded and partnerships with the private sector strengthened."

Following from the participants' insights and the analysis presented in this paper, we propose the following recommendations:

1

Better map the cyber ecosystem and understand its fragility as seemingly benign instances can have a 'butterfly effect' and cause maximum damage to diplomacy and economics.

For example, the tools of cyberspace allow for information, often disseminated in real-time, to be easily manipulated and turned into disinformation. Recognizing how the free flow of information, accessed by citizens as a democratic right is exploited by adversarial actors to undermine democratic systems, is essential.

2

Manage hyper-connectivity to make the internet a more trusted space: in order to protect democracies and citizens' data, better infrastructure and basic cybersecurity mechanisms need to be in place to prevent IT-enabled and denial- of-service attacks.

This includes an increased responsibility of tech companies, premised on a robust discussion on how this can be balanced with liberal freedom.

3

Build up leadership clusters amongst like-minded value partners to counter an adversary's efforts at undermining the international norms framework, similar to 5 Eyes concerted attribution efforts.

Increased cooperation would also be beneficial in the areas of Threat Information Exchange and Critical Infrastructure Protection.

4

Establish an internationally agreed-upon vocabulary which sets the basis for cooperation in an international norms framework.

Diplomatic initiatives to bolster cyber norm processes should be aimed at establishing enforceable rules rather than just models for good governance. This includes clearly articulated thresholds, denominators and escalation processes as well as commonly established consequences.

5

Set a distinct outline of deterrence, especially via offensive capabilities, premised upon an unambiguous definition of cybersecurity that is used as a common foundation.

Building up deterrence capabilities, even in their defensive form as 'deterrence by denial', requires innovation. This includes a shoring up of the cyber workforce to meet the demands of the future.

Appendix: Participant Contributions

"What Does Effective Deterrence In Cyber Space Look Like?"

"What Is The Best Approach on Effective Cyber Deterrence and which Course Of Action Should Be Recommended?"

***by* Lieutenant-General (ret'd) Kurt Herrmann**
President of the Clausewitz-Society, former Director of NATO Communication and Information Systems Services Agency (NCSA)

According to the findings of Clausewitz on strategy, the basic intent of defence is to impose our resisting will on an opponent so that he recognizes his aggressive efforts are hopeless or that he would have to pay a price far above his original expectations.

Deterrence is a general strategy intended to dissuade an adversary from taking an aggressive action not yet started. Particularly, deterrence is determined to discourage an aggressor's intent through instilling doubt or fear of the consequences. Deterrence theory gained increased prominence as a military strategy during the Cold War with regard to the use of nuclear weapons. A basic prerequisite for credible deterrence is the defenders capability to protect his forces against destruction which could be executed by a surprise attack.

Cyber attack capabilities are reality and we have to recognize that these capabilities could increasingly become a strategic instrument of inter-state conflicts. Meanwhile, the cyber domain is established as the fifth domain of security policy and warfare, on an equal footing with the domains land, air, sea and space. As cyber strongly permeates the four other domains, the vulnerabilities and potential threats posed by cyber attack capabilities can act as explosive crisis boosters. On the other hand, cyber capabilities are to be classified as catalysts for the development and employment of classic warfare capabilities. They act like force enhancements or power amplifiers. Particularly in hybrid threat scenarios, the operational cyber and information defence domain incorporates and provides all the features of a comprehensive networked security approach within a fully integrated combined and joint warfare environment.

The concept of deterrence in modern hybrid or cyber scenarios can be defined in analogy to the above mentioned as the demonstration of comprehensive defence capabilities by one party to convince another party to refrain from initiating some course of aggressive action. Deterrence – comprising a cyber defence capability as integral element – needs to convince a potential aggressor not to carry out the intended action because of the costs and losses he would have to incur. Specifically, the defender needs to acquire and credibly sustain a cyber defence capability which ensures the protection of critical infrastructure and resilience of his forces against any denial of vital services in case of a cyber surprise attack.

Today, a successful state-of-the-art deterrence policy must consider the whole spectrum of political, diplomatic and military terms. According to this, a successful comprehensive deterrence requires that a country, an Alliance or a coalition preserves its ability to retaliate, either by responding before its own capabilities are paralyzed or destroyed, or by ensuring a second strike capability.

Today, a successful state-of-the-art deterrence policy must consider the whole spectrum of political, diplomatic and military terms.

In hybrid scenarios, the boundaries between external and internal security dissolve. Therefore, a comprehensive deterrence should include all relevant security and defence capabilities; cyber security and defence capabilities need to be an integral component of this as well.

Early warning capabilities are most essential for effective deterrence. To develop early warning capabilities in the cyber and information domain still appears to be a huge challenge as follows:

Situational surprise in conflicts or wars normally has to be expected, both in terms of time and concentration of forces. Cyber attacks can be exerted with almost no pre-warning time, immediately, massively, with global cross-border potential, and fast as well as unpredictable concentration of forces. The complexity of potential actors and their motives as well as complex camouflage and deceived attacks complicate the attribution of cyber attacks considerably.

In the cost-to-means ratio, the cyber space, with its almost unlimited resources, proves to be highly effective, strategically relevant and particularly efficient for achieving politically defined ends or objectives. Consequently, cyber means – especially as integral parts of hybrid threats – will significantly change the target-means or cost-effect calculation in conflicts. Both, the impact assessment and the detection and assessment of damage from cyber attacks are extremely difficult and not very transparent. All in all, a really effective early warning capability is not yet available and the problem of attribution, which means identifying an attacker with sufficient reliability, is still largely unresolved.

Cyber capabilities of potential opponents are expected to remain hidden until their employment. And, as IT technology to a vast degree is dual-use technology, dynamically evolving proliferation of cyber capabilities is virtually unavoidable. Therefore, the creation and development of adequate responsiveness continues to be a specific challenge. Particularly, the focus must be on rapid detection and analysis of abilities, intentions and concrete effects of

potential opponents. Thus, joint intelligence, surveillance and reconnaissance as well as massively improved on-line forensic capabilities are considered to be priority tasks of cyber defence and predominantly of comprehensive deterrence. Resulting from the above, close cooperation with partners deems to be mandatory, in order to increase the number of sensors worldwide and consequently the volume of data which is a basic prerequisite for any kind of enhanced early warning capability. This needs to include capabilities for rapid intrusion detection, fast attribution based on high-performance forensic tools, and ultimately rapid response actions as well. And, not to forget adequate capabilities for collecting, fusing and exploiting a substantive, reliable situational picture, compiling adequate and all-comprising damage assessments, developing appropriate courses of defence action, and supporting rapid decision making for executing the necessary response actions without delay.

Analogous to the 'Joint and Combined Warfare' in the traditional warfare domains, the planning and conduct of cyber defence operations are to be also planned and implemented in the context of crisis management, conflict prevention or conflict resolution, as well as national or multinational collective defence. I regard it as significant to mention that cyber defence should not be regarded just as an add-on to conventional warfare. Rather, there is a strong need for fully integrating cyber defence in all phases and actions of comprehensive defence operations, from the early situational assessment, through the planning and decision making process, finally to the concrete operations in the field. More than in other operational domains, cyber defence requires a high level of creativity, flexibility, and responsiveness. Basically, the goal must be to ensure a maximum level of attack-prevention, and, if that should fail, to get from a detection of an attack as quickly as possible to an appropriate response.

All the above mentioned criteria need to be fulfilled in order to award a credible comprehensive deterrence. And, effective deterrence is closely linked to psychological elements and the assessment of rational behaviour. According to this, the credible demonstration of cyber deterrence capabilities appears to be quite a difficult task. Any disclosure of active or passive cyber defence capabilities could rapidly devaluate these capabilities, because opponents will be permitted to quickly adapt their own offensive or defensive capabilities. However, as cyber capabilities and operations in the cyber and information domain need to be fully integrated in a comprehensive approach on preventive security provisions and defence strategies, this holistic approach also needs to be applied to deterrence. Consequently, deterrence in cyber space should comprise a complex mix of deterrence capabilities from all operational domains, land, air, sea, space, and cyber. A potential opponent needs to be kept under uncertainty, how we would react on an aggression from his side. And, he should be provided a strong signal that he would have to pay a price far exceeding the value of any gains of an aggressive act from his side.

This kind of deterrence could be best arranged and provided by choosing an approach similar to the defence in depth approach already established in cyber defence structures of several states or organizations. Of course, the implementation will require considerable investments in complex, efficient cyber and also classical defence assets. But, as we are facing potential cyber threats of strategic dimensions, those investments would certainly be worth the effort.

Faced with growing risks and threats to security on the one hand and limited resources on the other hand, we witness an increased urgency for comprehensive cooperation between all parties and actors involved. Consolidated action of all relevant government resorts and close cooperation with international organizations involved are highly recommended. This needs to be extended to the area of comprehensive deterrence as well. Against the background of high evolution speed in the cyber space, the dynamic cycle of prevention and protection in cyber defence is considered crucial for effective defence preparedness.

High resilience and recoverability are paramount for avoiding denial of services and guaranteeing continued command and control on all levels of all vital areas. The establishment of sound structures reflecting the above mentioned features is also important for a credible comprehensive deterrence.

Deterrence in Cyber? Possible but Different

from Professor Mario Voigt
Professor of Digital Transformation and Politics
at the Quadriga University of Applied Sciences Berlin
Member of the State Parliament of Thuringia

Happy new year? Germans kicked off their new year with a widespread dissemination of hacked data belonging to celebrities and prominent political figures including chancellor Angela Merkel.

The stolen personal information, spreading via Twitter, included photos, chat logs, cellphone numbers, home addresses, emails, and more. The level of frequency and sophistication of cyber attacks, from alleged Russian subversion of the US 2016 presidential campaign, to Wannacry or Petya, is growing and has an increasing impact on politics, societies and economies. Despite a growing amount of academic and practitioner's attention, the question remains to how these kinds of activities can effectively be deterred.

Deterrence. Can it still work?

Incepting an idea is powerful. Since the end of the Second World War, in the midst of the Cold War dynamics and beyond the fall of the Soviet Empire, deterrence was seen as an appropriate strategy to prevent adversaries from taking specific actions, because the potential attacker's would be discouraged by the other's defense, and would be restrained by the fear of retaliation. Security was incepted and resting in the minds of the potential opponent. But does deterrence can still handle the nuances of the cyber space and the digital age?

At least, three aspects challenge the deterrence strategy.

First of all, times are changing. Neither the bipolar international system of the Cold War nor a pure American dominance does exist anymore. It has been replaced by a diversity of actors and threats involved. Today, more than 30 nation-states have cyber attack capabilities. Sophisticated digital toolkits are spreading like wildfire ranging from several nation-state with their excellent cyber capabilities like China or Russia to non-state actors like criminal groups or terrorist organizations. The European Network and Information Security Agency (ENISA) identifies six threat agents, namely corporations, cyber criminals, employees, hacktivists, nation states and terrorists, while the NATO CCD-COE study adds state-sponsored agents as a seventh actor.[1] They all have the ability to wage campaigns to seriously damage or disrupt critical infrastructure, cripple businesses, or attack devices used every day, without ever physically crossing a nations border. In fact, these cyber attacks offer potential adversaries' low cost and almost complete deniability.

Secondly, these state and non-state actors in cyberspace provide an asymmetric environment with unique characteristics, where concepts such as geography and sovereignty, military sphere and civilian sphere become blurry.

Finally, given a diverse landscape of (potential) adversaries and a very complex threat assessment, classical deterrence requirements such as defined interests and drawn redlines are under constant scrutiny. How to proceed against private agents but presumably state-sponsored? This leads to shifts in security fundamentals.

Given the disparate actor and threat environment, where private and public spheres mingle, sovereignty and domains become blurry, democracies have to innovate their strategic thinking when it comes to cyber deterrence and think bigger. A more holistic approach is needed, which recognizes cyberspace as a strategic environment with distinct dynamics.

In fact, deterrence seeks at its core to preserve the 'status quo' by persuading adversaries not to do something. However, in a cyber age insidious state or non-state actors continue to leverage all facets of the cyberspace in a dynamic, proactive fashion to achieve a fundamental shift in global power toward their advantage.

Research scholars appear divided if the deterrence still applies in cyberspace. Joseph Nye recently specified four key mechanisms for cyber deterrence: denial, punishment, entanglement, and norms.[2] Others do not see in deterrence a credible strategy anymore, because cyber is an entirely new strategic environment, one which has important distinctions from the traditional domains of land, sea, air, and space.[3] But how can democracies operate in such environment and respond accordingly?

Holistic Approach: Keep Initiative

Given the disparate actor and threat environment, where private and public spheres mingle, sovereignty and domains become blurry, democracies have to innovate their strategic thinking when it comes to cyber deterrence and think bigger. A more holistic approach is needed, which recognizes cyberspace as a strategic environment with distinct dynamics. Three dimensions come to mind.

At the core lays the gap between policy and technology. Cyberspace is an operational environment of constant action, permanent contact and ongoing contests with adversaries. While every new version of software or hardware can shift tactical capabilities, the interconnectedness of the cyberspace demands persistence – the gaining and retention of initiative.[4] In such a dynamic thinking Democracies need agile policies which allow for offensive and defensive measures as well as anticipating and integrating the technological change coming. Defending forward with persistence and active engagement will guide a deterrence by retaliation, which holds adversaries accountable and impacts their risk calculus.

Moreover, a comprehensive approach of cyber security emphasizing resilience will include private and public actors in unique way. In most democracies the private sector owns infrastructure and data, has the biggest cross-national interdependence and is conceptional better equipped for the cyber age. Building resilience and focusing on the cyber ecosystem is part of a deterrence by denial, which includes capacity building, shared incident reporting and response, expanding quantity and quality of digitally literate people, technological research and development. Hence, collaboration has to be expanded and partnerships with the private sector strengthened.

Finally, weak cross-national cooperation and diverging legislation stacks the deck in favor of attackers. In Europe, more than one third of the cyber security strategies of the countries are older than four years, but 17 of 29 strategies believe in international cooperation.[5] Hence, democracies have to promote democratic norms, creating an international framework for stability by defining clear global rules on acceptable practices and appropriate responses after attacks like criminal prosecution, economical sanctions or active retaliation. Though, there will be no easy blueprint. In their race for digital supremacy China and the U.S. will provide alter-native narratives on liberal norms, standards and protocols as preferred by Europe or other countries in Asia.[6] If Europe does not define its future role as a colony in the American tech empire than it has to become a more serious security and defence actor. Europe has to actively engage countries like Australia, India and other countries across Asia to shape progress in the international cyber agenda.

Old habits die hard, and outdated thinking harder still. Deterrence in a cyber age means an operational environment and strategy of constant action, permanent contact and ongoing contests with adversaries. Hence, the global digital ecosystem demands not just a pure military response. Recent attacks like in Germany proved a more holistic, even international, approach is needed including a range of political, social, economic, technological and legal responses. Security is achieved through imposed norms, clear expectations of state behavior, cooperation with non-state-actors, on an international level, but also a cyber initiative mindset. Deterrence, yes but different.

References

1. Ziolkowski, K. (ed.) (2013), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn.
2. Nye, J. S. Jr. (2016/7), "Deterrence and Dissuasion in Cyberspace", in: *International Security*, Vol. 41 No. 3, pp. 44–71. In his classical study, Lawrence Freedman differentiates 1) deterrence-by-retaliation and deterrence-by-denial; 2) immediate vs. general; 3) narrow vs. broad; and 4) central vs. extended deterrence, see: Freedman, L. (2004), *Deterrence*, Cambridge.
3. Fischerkeller, M.P., and Harknett, R.J. (2017), "Deterrence is Not a Credible Strategy for Cyberspace", *Orbis*, Vol.61 No.3, pp.381-393.
4. Fischerkeller, M.P., and Harknett, R.J. (2017), "Deterrence is Not a Credible Strategy for Cyberspace", *Orbis*, Vol.61 No.3, pp.381-393.
5. Deloitte (2018), European Cyber Defense, Strategies and Status Quo 2018, Berlin.
6. Heinl, C. (2018), Activities in the Asia Pacific related to Cyber Diplomacy: A consideration of EU involvement in shaping discussions, see: https://caitrionaheinlcyberpolicywatch.wordpress.com/2018/11/23/activities-in-the-asia-pacific-related-to-cyber-diplomacy-a-consideration-of-eu-involvement-in-shaping-discussions/

Dr. Thomas Fitschen

Ambassador, Special Representative for Cyber Foreign Policy and Cyber Security, German Federal Foreign Office

What is often simply called 'attribution' of a malicious cyber operation – or even simpler 'name and shame' – is actually a fairly complicated, multi-layered process. It is not a mathematical operation, but the assessment of a situation with lots of variables and few certainties.

At the initial level attribution requires a process (often called 'cyber forensics') that tries to establish the technical (IT-)facts. What is it that we see going on in our systems? Where does the malicious code come from, and can we identify the way it got here? Can we find an IP address, a server, the PC that was used? And what exactly is the 'damage', if any? That is often terribly difficult to ascertain, but not always outright impossible. At another level you would have to figure out who did it – is there an identifiable person who hit the 'enter' button?

As the vast majority of cyber incidents are being orchestrated by private individuals – for criminal or whatever other purposes – those are cases for our police and justice institutions. Countries like Australia and Germany have an elaborate system of norms that make 'cyber crime' of all sorts punishable under their national penal laws; we don't call it 'naming and shaming', but simply prosecution of a crime.

If the country concerned has sufficient reason to believe, however, that the perpetrator was the agent of a foreign state and that the operation violated international law, it will have to determine how to react – whether or not to confront the foreign government suspected of having orchestrated the operation, publicly or through what is known as 'diplomatic channels'. This is how international lawyers understand 'attribution'. As a term used in the context of the international law of State responsibility, attribution is the practice of assigning responsibility to a specific actor for a cyber operation which is perceived to constitute an internationally wrongful act. Different methods and procedures to attribute cyber operations and different definitions and criteria to establish a sufficient degree of certainty in attributing a cyber operation may be employed.

Legally speaking there is nothing new about it, but in an argument about the 'attribution' of a cyber operation it is a lot more difficult to make one's case, not least because much of the information that would back one's own assessment is classified and cannot be disclosed easily. As to the possible means for a reaction, international law provides a vast array of countermeasures, to be utilized in a calibrated, proportionate and effective way. The decision to go down that road, ideally together with partners and allies who are equally affected, is in any case the sovereign prerogative of the government. It is an intrinsically political act. In view of the legal and political difficulties involved, Germany and Australia have for many years engaged in activities at the UN to advance a common understanding of the international law that applies to such cases, and have advocated for clearer norms of responsible state behavior in cyberspace, confidence building measures and capacity building.

KONRAD ADENAUER STIFTUNG

Contact

Konrad Adenauer Stiftung (Australia) Limited
Regional Programme Australia and the Pacific
11/3 Sydney Avenue
Barton, ACT 2600
Australia
Tel: +61 2 6154 9322

Follow us:

www.kas.de/australia
www.facebook.com/KAS.canberra
www.linkedin.com/company/konradadenauerstiftungaustralia