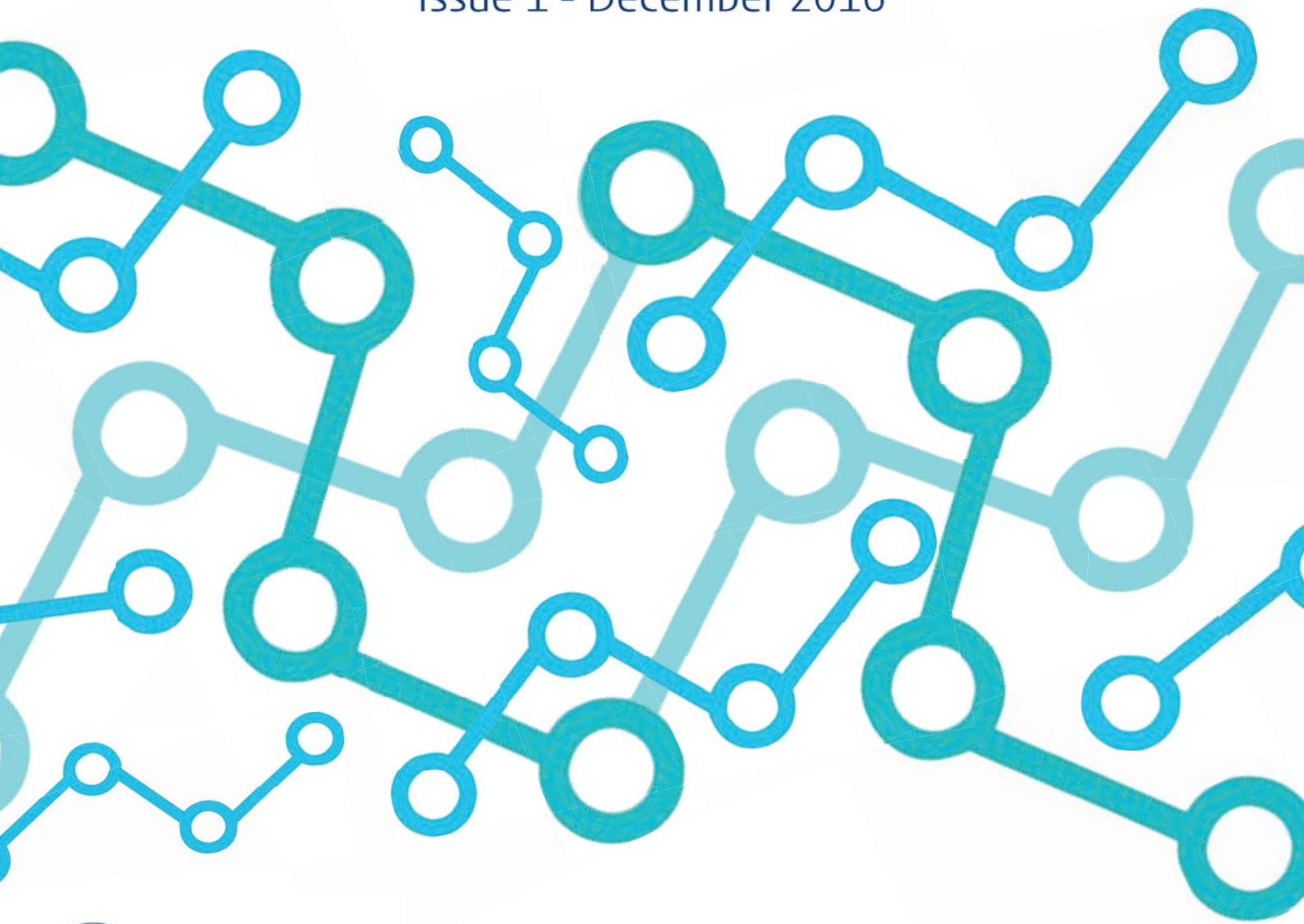
Promoting and protecting cyber security interests

Ducheine, P.

Publication date
2016
Document Version
Final published version
Published in
Journal of Security and Global Affairs

Journal of Security and Global Affairs

Issue 1 - December 2016



Universiteit Leiden
The Netherlands

Special Conference Issue:
Who determines the security (research) agenda?

Institute of Security and Global Affairs

E-ISSN 2452-056X

Journal of Security and Global Affairs

The Journal of Security and Global Affairs (SGA), published in open access by the Institute of Security and Global Affairs at Leiden University, is a refereed publication, and manuscripts go through a blind review process. The focus of SGA is on a wide array of security topics and issues, providing a platform for the analysis of key issues within security and global affairs. In doing so, SGA aims to generate new ideas and improve the management of safety and security. These include, but are not limited to, items pertaining to the terrorism and counterterrorism, cyber security and cybercrime, political violence, innovative practices, policy development and implementation, evaluative research and the (global) players engaged in these enterprises. Taking a multidisciplinary approach, SGA seeks to facilitate the exchange of knowledge and good practice. SGA publishes original articles that utilize a broad range of methodologies and international perspectives when examining pressing issues in safety and security across the globe.

Journal of Security and Global Affairs (ISSN 2452-0551, E-ISSN 2452-056X)

Special Issue Institute of Security and Global Affairs Conference Leiden University

This Special Issue of the Journal of Security and Global Affairs features the outcome of several workshops and lectures presented during the Institute of Security and Global Affairs Conference 'Who determines the security (research) agenda?' which was held on 9-10 November 2016 in The Hague, The Netherlands.

Facing contemporary security and global affairs challenges such as terrorism, cyber-attacks and hybrid warfare requires dialogue and collaboration between various disciplines within academia, as well as between academia and other stakeholders in the public and private sector. Such collaborations raise new questions and dilemmas, for instance about roles and responsibilities of stakeholders. One of the most important questions is what security issues or challenges to focus on and who should take the lead? The Leiden University's Institute of Security and Global Affairs (ISGA) focused on these questions during its opening conference. ISGA welcomed more than 200 actors from the security and global affairs field to discuss the central question 'Who determines the security (research) agenda?'. More information on the conference and a digital booklet full with pictures can be found here.

Promoting and protecting cyber security interests

Prof. dr. Paul Ducheine

Professor of Cyber Security and Cyber Operations University of Amsterdam, Professor Cyber Warfare Netherlands Defence Academy

1. Vital interests

For the Kingdom of the Netherlands six vital or strategic interests are at stake according to its national and international security strategies: territorial integrity, physical, economic and ecological security, social and political stability and a stable and effective international legal order. Due to developments in information and communication technologies, social behaviour, public as well as private, changed dramatically over the last decades. The Internet of things is just one of these examples of evolution in this respect. These changes impact on the Netherlands' vital interests (DESI, 2016). Apart from acknowledging the relevance of cyber security as essential for national security, demonstrated by the promulgation of two thematic National Cyber Security Strategies (I and II), we are actually conceding that cyber security has become the seventh vital interest for the Kingdom.

2. Threats and countermeasures

Threats to cyber security originate from a diversity of actors and, quite obvious, for various motives ascribed to those actors. Those actors, which may involve state and non-state entities - including the persons involved ('hackers') - will be inspired or driven by motives ranging from enhancing security on the one hand, to testing, training, boasting, activism, economic profit, sabotage, propaganda, subversion, theft, terrorism, espionage and (military) conflict on the other (Ducheine, 2015).

These threats require a multidisciplinary response, a comprehensive effort by public as well as private partners. These response are now formulated in Cyber Security Strategies worldwide.[1] The paradigms offer distinguishes framework for public and – were applicable – private organisation to promote and protect cyber security interests. Looking at cyber activities at the state level, a number of distinct paradigms are applicable to describe cyber operations (Klimberg & Mirtl, 2013). These paradigms are demonstrated in national cyber security strategies worldwide (CCD CEO, 2014), as well as through the instrumental use of cyber capabilities in furtherance of states' (other vital) interests.[2] These paradigms can be depicted as parts of a continuum, a spectrum, or to put it differently, as part of a state's comprehensive efforts in cyberspace (AIV & CAVV, 2011). The paradigms are complementary

[2] E.g. the use of Stuxnet against Iran.

and overlapping.[3] These paradigms represent one (or more) of the institutional frameworks enabling governments (or public authorities) to conduct activities within democratic societies. They thus offer a legal and social framework for (governmental) behaviour, that is, as with all social interaction, subject to adjustments that are initiated or inspired by changes in the security landscape (including 'new' threats), public opinion, international, societal and technological trends. As such, these frameworks reflect the *Zeitgeist* regarding topics that have reached the political agenda and require or enable governmental action (Rothman & Brinkel, 2012).

3. Imperfections and conflict of interests

For public bodies operating under the rule of law, legislation authorising and tasking these bodies is required as soon are governmental action impact upon citizens' rights and privileges. Inevitably, legislation in each of the paradigms may be incomplete and lagging behind social behaviour and technological opportunities. The legislator, enabling the executive branch by providing tasks and powers, is the pinnacle of the balance of conflicts between three interrelated perspectives. Firstly, security demands or ambitions require tasking accompanied by powers. Secondly, security comes at a price: either financially trough taxation to through infringements on other rights or privileges (i.a. privacy), as these security providing bodies require manpower, funds and powers. Thirdly, security offers benefits, as economy, society and social behaviour gain from security. Economic prosperity and individual or collective wellbeing may be the result of a secure place to do live and to do business.

4. In the discussion (Q&A): Cyber warfare

It is evident that cyber warfare proper should be reserved for the paradigm of military conflict.[4] Cyber warfare involves 'warfare proper' and 'operations other than war', including peace support (and enforcement) operations related to conflict (Gill & Fleck, 2015). Thus 'cyber warfare' can be defined as "employment of cyber capabilities with the primary purpose of achieving [military] objectives in or by the use of cyberspace" (Schmitt, 2013).

In response to cyber threats, cyber warfare is the *ultimum remedium*, and highly unlikely, as the other paradigms will prevail. However, as of now, most, if not all military operations abroad will be supplemented with cyber capabilities of some kind.

[3] Klimberg and Mirtl p 15, referring to these paradigms as 'mandates'.

References

AIV & CAVV (2011). Cyber Warfare (report no. 77/22, 2011), viewed 31 December 2012, www.aiv-advice.nl

CCD CEO (2014). 'National Strategies & Policies', *NATO Cooperative Cyber Defence Centre of Excellence*, viewed https://www.ccdcoe.org/328.html

Desi (2016). EU's Digital Economy & Society Index (DESI), viewed https://ec.europa.eu/digital-single-market/en/desi

Ducheine, P.A.L. (2015). 'The Notion of Cyber Operations in International Law', in: Nicholas Tsagourias & Russell Buchan (eds), *The Research Handbook on the International Law and Cyberspace* . Cheltenham: Edward Elgar Publishing

Gill, T.D. & Fleck, D. (2015). The Handbook of the International Law of Military Operations. Oxford Univesity Press: Oxford.

Klimberg, A. & Mirtl, P. (2013). 'Cyberspace and Governance—A Primer', *Austrian Institute for International Affairs* , viewed 11 November 2013, http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/Cyberspace_and_Governance_ _Working_Paper_65_2.pdf

Rothman, M. & Brinkel, T. (2012). 'Of snoops and pirates: Competing discourses of cybersecurity' in Paul A.L. Ducheine, Frans Osinga and J. Soeters (eds), *Cyber Warfare: Critical Perspectives* . The Hague: TMC Asser Press.

Schmitt, M. N. (2013). Tallinn manual on the international law applicable to cyber warfare : prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press.