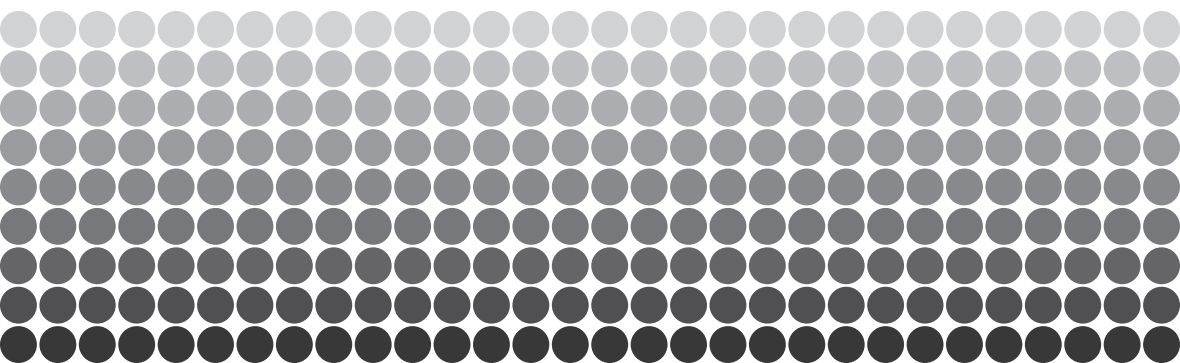
sipri

SIPRI YEARBOOK 2013

Armaments, Disarmament and International Security

Cybersecurity and the arms industry

VINCENT BOULANIN



sipri

STOCKHOLM INTERNATIONAL
PEACE RESEARCH INSTITUTE

Cybersecurity and the arms industry

VINCENT BOULANIN

Contents

This is an offprint of section II of chapter 4 of

SIPRI Yearbook 2013: Armaments, Disarmament and International Security
Oxford University Press, 2013, ISBN 978–0–19–967843–3, hardback, xxii+574 pp., £100/$185

The SIPRI Yearbook is published and distributed in print and online by Oxford University Press—more information is available at <http://www.sipriyearbook.org>

OXFORD
UNIVERSITY PRESS

www.sipriyearbook.org

II. Cybersecurity and the arms industry

VINCENT BOULANIN

The growing importance of cybersecurity in the military and civil realms has led to noteworthy diversification by arms production and military services companies into the cybersecurity market. This section presents a brief overview of cybersecurity, provides provisional information on the size of the cybersecurity market and reviews the involvement of arms-producing and military services companies in this market.

The rise of cybersecurity as a national security issue

Cybersecurity is defined and understood in different ways.[1] In a narrow and technical sense, cybersecurity has been defined as 'the ability to control access to network systems and the information they contain'—thus, strictly referring to the protection of cyberspace itself.[2] Security objectives are then traditionally framed in terms of preserving the confidentiality, integrity and availability of cyberspace.[3] The cybersecurity concept has also gained a national security dimension as the public, businesses and the military have become increasingly dependent on computer and networked technologies—in fact, it has been 'securitized'.[4] Hence, within the political realm, cybersecurity deals with the challenges produced by cyberspace as a new medium for threatening activities (e.g. criminality, terrorism, espionage or warfare) and the belief that a lack of cybersecurity might affect the security of the economy, the state and society in general.[5] From an industry perspective, cybersecurity has been defined as 'an emerging field of protecting computer systems and data from interference through the Internet'.[6]

[1] The adjective 'cyber-' and the concept 'security' are themselves objects of definitional controversy. On the definition of cybersecurity see e.g. Dunn Cavelty, M., 'Cybersecurity', ed. P. Burgess, *The Routledge Handbook of New Security Studies* (Routledge: New York, 2010), pp. 154–55.

[2] Bayuk, J. L. et al., *Cyber Security Policy Guidebook* (John Wiley: Hoboken, NJ, 2012), p. 1. 'Cyberspace' has been defined as 'the combination of the virtual structure, the physical components that support it, the information it contains, and the flow of that information within it'. Fischer, E. A., *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, Congressional Research Service (CRS) Report for Congress RL32777 (US Congress, CRS: Washington, DC, 22 Feb. 2005), p. 5.

[3] Nissenbaum, H., 'Where computer security meets national security', *Ethics and Information Technology*, vol. 7, no. 2 (June 2005), p. 63.

[4] On securitization see Buzan, B., Wæver, O. and de Wilde, J., *Security: A New Framework for Analysis* (Lynne Rienner: Boulder, CO, 1998), p. 25; and Hansen, L. and Nissenbaum, H., 'Digital disaster, cybersecurity and the Copenhagen School', *International Studies Quarterly*, vol. 53, no. 4 (2009), pp. 1155–75.

[5] Hansen, L. and Nissenbaum, H., 'Digital disaster, cyber security, and the Copenhagen School', *International Studies Quarterly*, vol. 53, no. 4 (Dec. 2009), pp. 1155–75.

[6] EADS, *EADS Annual Review 2011: Progressing, Innovating, Transforming* (EADS: Leiden, 2012), p. 64.

The 'securitization' of cyberspace—that is, the process that transformed the security of cyberspace into a national security concern—began in the late 1980s, focusing first on issues of military relevance. As individual states began to rely increasingly on network systems for the management of weapon platforms and critical infrastructure, military institutions also began to identify the threat of cyberattacks that could paralyse arsenals or lead to leakages of strategic information. Subsequently, these institutions began developing both defensive and offensive capacities to take action within cyberspace. For some analysts, cyberspace has since become a fourth 'battle space'—after air, land and sea.[7]

In the 1990s, as economic activities and social infrastructures became increasingly reliant on Internet and networked technologies, the securitization process accelerated and gained a civil dimension (i.e. it became a national security issue beyond the traditional military sense).[8] Information technology (IT) experts and security analysts observed vulnerabilities arising from the interconnectivity of computer systems, warning of the cascading effects of cyberattacks on the economy and society—and, therefore, on national security.[9] An accumulation of small and relatively simple attacks targeting companies, governments and private persons (e.g. phishing, fraud or espionage) may cause major losses for national economies, while major targeted cyberattacks have the potential to significantly disrupt society's smooth functioning. For instance, cybersabotage leading to the disruption of national or local electric power systems would 'involve at least opportunity costs—interruption of business, forgoing of various activities and associated benefits'.[10]

While no major cyberdisaster—or 'electronic Pearl Harbor'—has yet occurred, several events in recent years have reinforced the credibility of such scenarios, leading to political and institutional responses from international and national security communities.[11] Notably, the Estonian

[7] Rid, T., 'Cyber war will not take place', *Journal of Strategic Studies*, vol. 35, no. 1 (Feb. 2012), pp. 5–32.

[8] Dunn Cavelty, M., *Cyber-security and Threat Politics: US Efforts to Secure the Information Age* (Routledge: London, 2008), p. 2.

[9] From a technical perspective, cyberattacks can be classified according to their ability to (*a*) destabilize, e.g. through a denial of service (DoS) attack; (*b*) spy and control, e.g. through use of a trojan horse; or (*c*) destroy, as in the case of the Stuxnet virus. On the political dimensions of cyberattacks see Deibert, R. J. and Rohozinski, R., 'Risking security: policies and paradoxes of cyberspace security', *International Political Sociology*, vol. 4, no. 1 (Mar. 2010), pp. 15–32; and Dunn Cavelty, M., 'Cyberwar: concept, status quo and limitations', Centre for Strategic Studies (CSS) Analysis in Security Policy no. 71, Apr. 2010, <http://www.css.ethz.ch/publications/CSS_Analysis_EN>, pp. 1–2.

[10] US National Research Council, Computer Science and Telecommunications Board, *Cybersecurity Today and Tomorrow: Pay Now or Pay Later* (National Academy Press: Washington, DC, 2002) p. 6; and Andersson, R. H. and Hearn, A. C., *An Exploration of Cyberspace Security R&D Investment strategies for Darpa: "The Days After . . . Cyberspace II"* (RAND: Santa Monica, CA, 1996).

[11] The term 'electronic Pearl Harbor' was allegedly coined in 1991 by Winn Schwartau during testimony before the US Congress. See Schwartau, W., *Information Warfare: Cyberterrorism: Pro-*

Government and its agencies were victims of a large-scale cyberattack in 2007.[12] Portrayed as the 'first war in cyberspace', this incident eventually led Estonia and nine other EU member states to adopt national cybersecurity strategies.[13] It also prompted the North Atlantic Treaty Organization (NATO) to adopt a policy on cyberdefence, under which it created a cyberdefence management authority and supported the creation of a cooperative cyberdefence centre of excellence in Tallin, Estonia, in 2008.[14] In the United States, President Barack Obama has made cybersecurity a priority of his presidency.[15] In 2010 the US Army established the US Cyber Command (USCYBERCOM) and in 2011 the US Department of Defense published a new cybersecurity strategy, colloquially known as Cyber 3.0.[16]

In 2012 cybersecurity continued to rise on the agendas of the international political and security communities. Revelations about Flames and Stuxnet—two viruses described as Western cyberweapons targeting Iran—made headlines and inspired fresh discussions about the growing use of cyberweapons and cyberwarfare.[17] While there is no reliable evidence, a growing number of countries—including China, Iran, Israel, Russia and the USA—were suspected of using cyberweapons and making offensive interventions across cyberspace.[18] In that context, at the 2012 Security Jam, officials from NATO and the EU and researchers from top European think tanks discussed the need for global governance in cyberspace.[19] At the

tecting Your Personal Security in the Electronic Age (Thunder's Mouth Press: New York, 1994), p. 43; and Bendrath, R., 'The American cyber-angst and the real world: any link?', ed. R. Latham, *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security* (New Press: New York, 2003), p. 50.

[12] A list of major cyber incidents since 2006 has been compiled by the Center for Strategic and International Studies (CSIS). Lewis, J. A., 'Significant cyber events', <http://csis.org/publication/cyber-events-2006/>.

[13] Landler, M. and Markoff, J., 'In Estonia, what may be the first war in cyberspace', *New York Times*, 28 May 2007. The 9 other EU member states that have adopted cybersecurity strategies are Finland (in 2008), Slovakia (2008), the Czech Republic (2011), France (2011), the UK (2011), Germany (2011), Lithuania (2011), Luxembourg (2011) and the Netherlands (2011). European Network and Information Security Agency, 'National cyber security strategies: setting the course for national efforts to strengthen security in cyberspace', May 2008, <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper>.

[14] North Atlantic Treaty Organization (NATO), Cooperative Cyber Defence Centre of Excellence (CCDCOE), 'About', [n.d.], <https://www.ccdcoe.org/3.html>.

[15] White House, 'Remarks by the President on securing our nation's cyber infrastructure', 29 May 2009, <http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure>.

[16] US Department of Defense (DOD), *Department of Defense Strategy for Operating in Cyberspace*, (DOD: Washington, DC, July 2011).

[17] Kaspersky Lab, 'Kaspersky Lab and ITU research reveals new advanced cyber threat', 28 May 2007, <http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Research_Reveals_New_Advanced_Cyber_Threat>.

[18] Perlroth, N., 'Hackers in China attacked The Times for last 4 months', *New York Times*, 30 Jan. 2013; and Sanger, D. E., 'Obama order sped up waves of cyber attacks against Iran', *New York Times*, 1 June 2012.

[19] Of the 2012 Security Jam's 10 recommendations, 2 concerned cybersecurity: recommendation 6 proposed 'confidence-building measures for cyber global governance', while recommendation 7 con-

national level, the US Senate discussed the adoption of a comprehensive cybersecurity act, while the French Senate published a report calling for cyberdefence and information network protection to be made national priorities, as well as a public doctrine for offensive capacity within cyberspace.[20]

Two notable developments in cybersecurity occurred in early 2013. First, in February 2013 the European Union published its cyberspace strategy.[21] Second, in March 2013 US officials stated that cyberattacks have now replaced al-Qaeda as the greatest threat to US national security.[22]

The cybersecurity market and the arms and military services industry

The rise of cybersecurity on the political and military agenda has evident economic implications. Globally, public and private cybersecurity spending was estimated to be approximately $60 billion in 2011.[23] If accurate, this would be equal to 3.5 per cent of world military expenditure in 2011.[24] The USA was the number one spender on cybersecurity, accounting for half of the total, and was the only country where the levels of public and private spending on cybersecurity were almost equal.[25] In the rest of the world, the private sector accounted for the majority of national spending on cybersecurity.[26] With cybersecurity becoming a top national security concern, public demand is expected to experience sustained growth in the next

cerned the need to introduce hacker recruitment into public cybersecurity policy. See Dowdall, J., *The New Global Security Landscape: 10 Recommendations from the 2012 Security Jam* (Security and Defence Agenda: Brussels, 2012), pp. 17–19.

[20] US Senate, Homeland Security Committee, 'Cosponsors discuss revised Cybersecurity Act, S.3414, and the concessions made to win support for the legislation to address a threat that is well upon us', 24 July 2012, <http://www.hsgac.senate.gov/hearings/cosponsors-to-discuss-revised-cybersecurity-act-concessions-made-to-obtain-support-for-threat-thats-already-here->; and Bockel, J. M., *Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyber défense* [Report on behalf of the Committee on Foreign Affairs, Defence and Armed Forces on cyberdefence], Senate Report no. 681 (Sénat: Paris, 2012), pp. 96, 113–19.

[21] European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (European Commission: Brussels, 2013).

[22] Dilanian, K., 'Cyber-attacks a bigger threat than Al-Qaeda, officials say', *Los Angeles Times*, 12 Mar. 2013.

[23] PriceWaterhouseCoopers, 'Cybersecurity M&A: decoding deals in the global cybersecurity industry', Nov. 2011, <http://www.pwc.com/gx/en/aerospace-defence/publications/cyber-security-mergers-and-acquisitions.jhtml>, p. 5. These figures should be treated with caution, as they are rough estimates made by market research companies. Such companies tend to overestimate the size of the market and do not make public the methodology for their calculation.

[24] According to SIPRI estimates, world military expenditure in 2011 totalled $1738 billion. Freeman, S. and Solmirano, C., 'Global developments in military expenditure', *SIPRI Yearbook 2012*.

[25] PriceWaterhouseCoopers (note 23).

[26] PriceWaterhouseCoopers (note 23), p. 5; and Wagley, J., 'Report: cybersecurity market to almost double in five years', 7 Nov. 2012, <http://securitymanagement.com/news/report-cybersecurity-market-almost-double-five-years-0010070>.

decade.[27] According to some forecasts, the cybersecurity market should double in size by 2017, to about $120 billion.[28]

This strong growth—coupled with the actual and potential cuts in military spending in some key weapon markets—helps explain why many arms-producing and military services companies show increasing interest in the cybersecurity market. In 2012 major arms-producing companies continued to acquire cybersecurity providers (see table 4.2 in section I above).[29] Diversifying into cybersecurity enables these companies to widen their customer base into the civilian sector, while also developing technical competences for electronic warfare and cyberdefence for the military market.

Cybersecurity companies in the SIPRI Top 100

Leading system integrators (LSIs), IT companies and military services companies are the primary providers of cybersecurity products and services in the SIPRI Top 100 for 2011.[30] Almost all the major LSIs—including BAE Systems, the European Aeronautic Defence and Space Company (EADS), Finmeccanica, Lockheed Martin, Northrop Grumman, Raytheon, Saab and Thales—operate in the cybersecurity market, in some cases via specific divisions. However, these companies differ in terms of the strategies they have followed when establishing their respective cybersecurity businesses. For example, BAE has pursued an acquisition strategy in order to build its cyber and intelligence segment. It acquired Detica in 2008, Norkom Group and the Danish company ETI in 2010 and three divisions of L-1 Identity Solutions in 2011. In 2013 BAE also collaborated with Vodafone to develop security solutions for mobile communications.[31] In contrast, in 2012 EADS regrouped all of its existing cyber-related capacities in order to develop a specific cybersecurity business, while Lockheed Martin made strategic alliances with key IT and cybersecurity companies, such as Microsoft, Hewlett Packard (HP), McAfee and Cisco.[32]

[27] Wagley (note 26).

[28] PR Newswire, 'Cybersecurity market worth $ 120.1 billion by 2017', Wallstreet Online, 28 June 2012, <http://www.wallstreet-online.de/nachricht/4952697-marketsandmarkets-global-cyber-security-market-worth-120-1-billion-by-2017>.

[29] Acquisitions of cybersecurity providers by arms-producing companies are also discussed in e.g. Jackson, S. T., 'Key developments in the main arms-producing countries', *SIPRI Yearbook 2012*, pp. 228–29; and Boulanin, V., 'Major arms industry acquisitions, 2010', *SIPRI Yearbook 2011*, p. 264.

[30] Leading systems integrators are generally prime contractors in charge of leading major weapon programmes. They design and build major military systems by combining components, subsystems and software from multiples sources. Such companies constitute the upper end of the arms industry. See Gholz, E., 'System integration in the US defence industry: who does it and why is it important ?', eds A. Prencipe, A. Davies and M. Hobbey, *The Business of System Integration* (Oxford University Press: Oxford, 2005), pp. 281–82.

[31] BAE Systems, *Annual Report 2011* (BAE Systems: London, 2011); and Gribben, R., 'BAE and Vodafone partner for cyber-security market push', *Daily Telegraph*, 17 Feb. 2013.

[32] Trévidic, B., 'EADS Cassadian veut devenir un grand de la cybersécurité' [EADS Cassadian wants to become a giant of cybersecurity], *Les Echos*, 27 Apr. 2012; and Lockheed Martin, 'The

In addition, 10 of the 20 military services companies in the SIPRI Top 100 in 2011 provide cybersecurity solutions. Some of these companies—including HP, Computer Sciences Corporation (CSC) and CACI International—already specialized in IT-related services.[33] Others, such as L3 Communication, SAIC, QinetiQ and ManTech, specialize in the provision of national security-related services.

The lack of satisfactory data makes it difficult to evaluate and compare companies' cybersecurity-related revenues. In addition, arms-producing and military services companies tend not to report cybersecurity sales data unless it relates to specific cybersecurity divisions. When they do report such figures, companies usually do not differentiate between military and civil cybersecurity revenues. Available data suggests that cybersecurity remains a relatively minor source of revenue for LSIs. However, given the size of their total arms sales, this small proportion can still represent substantial revenue. For example, while only 7 per cent of BAE Systems' total revenue in 2011 was generated by its Cyber and Intelligence segment, this nevertheless represented £1.4 billion ($2.2 billion) in earnings.[34] Northrop Grumman reported that 30 per cent of its total revenues in 2011 came from its Information Systems division, while Lockheed Martin's Information Systems and Global Solutions division generated 20 per cent of the group's total sales.[35] In both cases, however, cybersecurity was just one activity among others for these divisions and neither company provided a further breakdown of revenues.

Cybersecurity provision and cybersecurity customers

Arms industry cybersecurity offerings consist primarily of services that can be divided into four main categories: network and data protection software and services; testing and simulation services; training and consulting services; and operational support (see table 4.3). While subcategories of services can also be identified, all of the LSIs and military services companies mentioned above provide 'solutions' (i.e. a combination of products and services) within these four categories. In most cases, companies set up a cybersecurity operations centre to provide these solutions in an integrated fashion.

Companies providing cybersecurity services target a wide range of customers. Public sector customers include the military, the intelligence com-

Lockheed Martin cyber security alliance', [n.d.], <http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-Cyber-Security-Alliance-Brochure.pdf>.

[33] HP first appeared in the SIPRI Top 100 after it acquired EDS in 2008. Jackson, S. T., 'Arms production', *SIPRI Yearbook 2010*, p. 280.

[34] BAE Systems (note 31), p. iii.

[35] Northrop Grumman, *Annual Report 2011* (Northrop Grumman: Falls Church, VA, 2011), p. 42; and Lockheed Martin, *Annual Report 2011* (Lockheed Martin: Bethesda, MD, 2011), p. 5.

Table 4.3. Main types of cybersecurity product and service by arms-producing and military services companies

Type of activity/ subcategories	Examples of companies
Network and data protection software and services	
Encryption solutions Identity management authentication solutions System configuration Data-loss prevention Malware defection and mitigation	BAE Systems, CACI, CSC, EADS, ManTech, Raytheon, SAIC
Testing and simulation services	
Penetration testing and vulnerability assessment Business/economic impact analysis Accreditation/technology compliance assessment	BAE Systems, CSC, EADS, Lockheed Martin, ManTech, SAIC
Training and consulting services	
Personnel training Consulting, including: infrastructure design, planning and implementation, cybersecurity policy definition	BAE Systems, CACI, CSC, EADS, Lockheed Martin, ManTech, SAIC
Operational support	
Network monitoring software and services Incident management, digital forensics and recovery solutions Incident response/counter-intrusion support Offensive cyberspace operations	BAE Systems, CSC, EADS, L-3 Communications, Northrop Grumman

Source: SIPRI Arms Industry Database and company annual reports and websites.

munity and other government agencies, while private customers include operators of critical infrastructure (e.g. energy suppliers, telecommunication companies, banks and hospitals) and other major companies. A number of LSIs (e.g. Lockheed Martin, BAE Systems and EADS) and major military services providers (e.g. CACI and ManTech) deal primarily with military and government agencies and, to some extent, major operators of critical infrastructure. These companies rarely provide standard cyber-solutions for companies whose activities have no direct national security relevance. For instance, in 2011 BAE's Cyber and Intelligence segment classed 91 per cent of its sales as government sales, and only 9 per cent as private commercial sales.[36] There are two possible explanations for this. First, while traditional arms producers have less experience in competing under commercial market conditions, they are more accustomed to dealing with large government contracts (both military and non-military). Their extensive contact with government customers also gives them an advantage

[36] BAE Systems (note 31).

in this sector of the market. Second, states have clearly indicated that cybersecurity will remain exempt from security-related budgets cuts. In contrast to LSIs and major military services providers, IT cybersecurity specialists such, as CSC and SAIC, have a wider customer base in the private sector.

Prospects and challenges

The expansion of arms-producing companies into the cybersecurity market is a clear trend in the first tier of the SIPRI Top 100.[37] These companies expect to benefit from long-term and increasing demand for cybersecurity services. The sustainability of this demand will depend on continued increases in the political, economic and strategic importance attached to cybersecurity, as well as the levels of public technical expertise and governments' political room to manoeuvre in this domain. While many Western states are actively recruiting cybersecurity experts the scarcity of this expertise, as well as the fast pace and technical complexity of cyberaffairs, means that these states may need to continue to rely on the private sector. Cybersecurity service providers commonly argue that they are better positioned to face cyber-related challenges. As national cyberinfrastructures—including fibre cable networks and relay antennas, as well as other critical infrastructure that might be targeted by cyberattacks, such as power plants—are generally not state-owned, but rather the responsibility of private actors, governments must also consider these actors as essential interlocutors in the implementation of their national cybersecurity policies. Some cybersecurity providers have even called for cybersecurity policy to be governed via public–private partnership (PPP) frameworks.[38]

However, in terms of the use of private security companies in warfare and other public security contexts, states' reliance on private cybersecurity providers could become a matter of political concern, particularly with regard to democratic transparency, oversight, accountability and cost.[39] Indeed, such outsourcing could be seen as a case of what Anna Leander has

[37] 'First tier' refers to the top of the arms production pyramid, which primarily includes prime contractors specializing in systems integration, major producers of sub-systems and major military services companies.

[38] Intelligence and National Security Alliance (INSA), *Addressing Cyber Security through Public-Private Partnership: An Analysis of Existing Models* (INSA: Arlington, VA, 2009); Grauman, B., *Cyber-Security: The Vexed Question of Global Rules* (Security and Defence Agenda: Brussels, 2012), pp. 32–34; and Dowdall, J., 'Public–private cooperation in cyber-security', Security and Defence Agenda (SDA) Policymakers' Dinner Report, Brussels, 30 Jan. 2012, <http://www.securitydefenceagenda.org/Contentnavigation/Activities/Activitiesoverview/tabid/1292/EventType/EventView/EventId/1097/EventDateID/1109/PageID/5428/Publicprivatecooperationincybersecurity.aspx>.

[39] On these issues see Buckland, B. S., Schreier, F. and Winkler, T. H., 'Democratic governance challenges of cyber security', Geneva Centre for the Democratic Control of Armed Forces (DCAF) Horizon 2015 Working Paper no. 1, 2010.

described as the 'privatization of the politics of protection'.[40] The provision of services by arms-producing companies—as well as traditional cybersecurity providers—may change the way in which states define and manage their cybersecurity and cyberdefence policies. Indeed, the services of cybersecurity companies help to shape the understanding and political reactions of public officials as they define threats and vulnerabilities (through the companies' testing and simulation and consulting services), interpret security situations (through the companies' consulting services) and suggest means to deal with them (through the companies' operational support services). More research remains to be done on the governance of the cybersecurity sector to understand and reflect on the actual involvement and responsibility of private companies in the design and implementation of states' cybersecurity and cyberdefence policies.

[40] In other words, the 'privatization of politics surrounding the definition of threats and the protection needed to secure them'. Leander, A., 'Privatizing the politics of protection: military companies and the definition of security concerns', eds J. Huysmans, A. Dobson and R. Prokohvnik, *The Politics of Protection: Site of Insecurity and Policy* (Routledge: New York, 2006), p. 19.