Społeczeństwo
i Polityka
Общество
и политика
Society
and Politics

Międzynarodowy Projekt Naukowy
Akademii Humanistycznej im. A. Gieysztora w Pułtusku
i Biszkeckiego Uniwersytetu Humanistycznego im. K. Karasaeva

International Scientific Project
of Pultusk Academy of Humanities named after A. Gieysztor
and Bishkek Humanities University named after K. Karasaev

Projet scientifique international
de l'Académie des Sciences Humaines A. Gieysztor de Pultusk
et l'Université des Sciences Humaines K. Karasayev de Bichkek

Международный Научный Проект
Гуманитарной Академии им. А. Гейштора в Пултуске
и Бишкекского Гуманитарного Университета им. К. Карасаева

AKADEMIA HUMANISTYCZNA IM. ALEKSANDRA GIEYSZTORA
WYDZIAŁ NAUK POLITYCZNYCH
AKADEMICKIE TOWARZYSTWO EDUKACYJNO-NAUKOWE „ATENA"

Społeczeństwo i Polityka
Общество и политика
Society and Politics

Redaktorzy tomu:
Maria Golińska-Wapińska
Kusein Isaev
Oliwia Piskowska

Nr 3 (40)/2014
Pułtusk

ISSN 1733-8050

Wydawca
Akademia Humanistyczna im. Aleksandra Gieysztora
Wydział Nauk Politycznych
ul. Spacerowa 7, 06-100 Pułtusk
tel./fax (23) 691-90-66
e-mail: piotrmotyka@interia.pl
www.pismosip.ah.edu.pl

Nakład 1000 egz
Objętość: 19.9 ark. wyd.

Wersja pierwotna: papierowa

Realizacja na zlecenie Wydawcy
Oficyna Wydawnicza ASPRA-JR

KIRGISTAN – POLITYKA I GOSPODARKA

TEORIA I METODOLOGIA NAUK SPOŁECZNYCH

BEZPIECZEŃSTWO PAŃSTWA

POLITYCZNE PROBLEMY EURAZJI

VARIA

RECENZJE, ESEJE RECENZYJNE, ARTYKUŁY RECENZYJNE

Contents

Contents

VARIA

REVIEWS, REVIEW ARTICLES, REVIEW ESSAYS

KIRGHIZISTAN – POLITIQUE ET ÉCONOMIE

THÉORIE ET MÉTHODOLOGIE DES SCIENCES SOCIALES

SÉCURITÉ DE L'ÉTAT

PROBLÈMES POLITIQUES DE L'EURASIE

VARIA

FICHES DE LECTURES, ESSAIS, COMPTE-RENDUS DE LECTURE

КЫРГЫЗСТАН – ПОЛИТИКА И ЭКОНОМИКА

ТЕОРИЯ И МЕТОДОЛОГИЯ ОБЩЕСТВЕННЫХ НАУК

БЕЗОПАСНОСТЬ ГОСУДАРСТВА

ПОЛИТИЧЕСКИЕ ПРОБЛЕМЫ ЕВРАЗИИ

VARIA

РЕЦЕНЗИИ, РЕЦЕНЗИИ-ЭССЭ, СТАТЬИ-РЕЦЕНЗИИ

Krzysztof Śliwiński

The Fifth Domain – national security in private hands? Civilianization of cyber security in United Kingdom

Introduction

A month before the Games of the XXX Olympiad, colloquially known as London 2012, Sir Jonathan Evans, the then chief of MI5 – British intelligence agency – warned that MI5 was battling 'astonishing' levels of cyber-attacks carried out by criminals and states alike against British internet vulnerabilities[1]. Even though the Olympiad as such did not prove as particularly fertile ground for the compromise of British cyber security, it did draw a lot of public attention as an event that could potentially prove its exposure to cyber attacks. As Sir Evans claimed, "what was at stake was not just British government secrets but also the safety and security of British infrastructure, the intellectual property that underpins Britain's future prosperity and ... commercially sensitive information"[2].

As of the beginning of the twenty-first century, the digital realm has decidedly entered our lives and brought profound changes to our existence. From individuals to private companies, civil society institutions to non-state agents, and national governments to supranational actors, the gathering, analysis, and release of all kinds of information relies to some extent on cyber-related media. This brings new challenges to how societies operate in general, but more specifically how governments perform their function as security providers. Traditionally defined as the only entities that possess a monopoly on the legitimate use of physical force, national governments around the world find themselves more and more challenged by the ongoing phenomena of the democratization of information. Without the ability to control the flow of information, democratic as well as non-democratic regimes face rising costs in maintaining the integrity of their political systems.

[1] *MI5 fighting "astonishing" level of cyber-attacks*, 25 June 2012, http://www.bbc.co.uk/news/uk-18586681, access: 05.2014.

[2] Ibid.

More specifically it has become a formidable task for liberal democracies to maintain a degree of nationwide security (with effects at both state and individual levels) in the era of cyber domains – a completely new, manmade level of social interaction based on a physical, electronic-operating infrastructure. Consequently there has been realization of the new level of threats that national security strategies should address in order to stay effective as primary tools of national security. With this, the concepts of cyber security, cyberspace, and cyber power have come to feature public policy decision making. In light of this, the fundamental question that emerges concerns the options that are left to states in their pursuit of national security strategies. More precisely, given the characteristics of the so-called 'fifth domain' (cyberspace), what can states do to address the seemingly inescapable paradox of security versus democratization of information?

This paper uses the case of the United Kingdom and its recent developments in the national security arena to address this conundrum. It principally introduces the notion of 'civilianization' of security in discussing the underlying problem of the effectiveness of states as providers of security amidst the freedom of information as an inherent feature of every democratic system of government. It is claimed that 'civilianization' of security is understood as non-military, voluntary organizations and the business/private sector engaged by government but acting in its own right to prevent, protect and prepare in the context of cyber strategy. It is conceived of as potentially an optimal tool to bridge the gap between two incompatible worlds of state security and personal freedoms.

The leading theoretical perspective evoked in this paper is the one presented by Ken Booth's postulate of emancipation of individuals as referent objects of security and the broader human security theorem, referring to the role of the state in serving and supporting the people from whom it draws, or should draw, legitimacy, rather than seeking its own security as an end in itself.

The first section of the paper sets the stage for the discussion by introducing the basic characteristics of cyberspace and its relevance to concepts such as power. The second section then introduces the notion of 'civilianization' of security with regards to cyber security, understood as protection of information and systems from cyber threats such as cyber terrorism, cyber warfare, and cyber espionage.

It continues with the analysis of United Kingdom responses to threats and challenges that emanate from cyberspace. Five major threats as identified by the British National Security Strategy are examined in a specific British context.

The paper concludes with the evaluation of the utility of the British response to cyber threats. It is claimed that British authorities have taken right steps in the right direction; however, much more needs to be done in terms of information and implementation. It is claimed that 'civilianization' of security in the fifth domain presents state authorities with a viable and potentially effective response to cyber threats, perhaps more than in any other domain. However, specific limitations in that area have to be kept in mind when designing public policies.

Old Concepts in the New Brave World – the Fifth Domain

Before analysing the specifically British response to otherwise global threats that emerge from cyberspace, a few introductory lines explain its meaning. Cyberspace is an entirely manmade 'space' that enables social interaction based on the material infrastructure[3]. Cyberspace makes the seemingly impossible, imaginable or even doable. For example, it is entirely plausible to carry out an espionage activity at a minimum cost and risk to the agents and the 'structure' they represent, be it a state or non-state[4]. It is feasible to access the adversary's major infrastructural network and plant 'logic bombs' (hidden instructions, often introduced with the Trojan horse technique, that stay dormant until a specific event occurs, at which time the instructions are activated) waiting to be triggered at an appropriate time without the target even knowing it[5]. This consequently means that numerous concepts that have been developed over the years regarding the tangible, physical world will not apply in the new non-physical reality or will need reconceptualising and redefining to fit the new realm[6].

One of the most important, perhaps *the* most important, notion for any political scientist is 'power'. Traditionally based on the realist approach, power has been defined as capabilities that can be quantified and converted into military strength. However, the end of the Cold War brought a plethora of new factors influencing an actor's power in IR amid interdependence and globalization. Writing at the beginning of the 21st century, Joseph Nye made a convincing case about the changing nature of world power and its reliance on other than only military sources in the global information environment[7].

The question that persists is: how do we define power in the 21st century when it is conceivable that one hacker can access, alter or even steal sensitive security related data without the owner of such information (governments and private companies) even being aware of such acts? How do we define the strength of the most influential states, such as the USA, if the level of their dependence on computer-run systems makes them more vulnerable and susceptible to (cyber) attacks than say, Somalia or Bhutan (with all due respect to their peoples)? How does the traditional thinking about power in terms of military capabilities fit into the picture of cyberspace?

---

[3] D.J. Betz, T.C. Stevens, *Cyberspace and the State: Towards a Strategy for Cyberpower*, London 2012, p. 35.

[4] L. Tabansky, *Basic Concepts in Cyber Warfare*, "Military and Strategic Affairs" 2011, no 3:1, p. 76–78.

[5] *Encyclopædia Britannica Online*, s. v., 'logic bomb', access: 05.2014, http://www.britannica.com/EBchecked/topic/741892/logic-bomb

[6] For example the case of terrorism in cyberspace – cyberterrorism. In reality, it is oftentimes difficult to distinguish between cybercrime, cyberterrorism and cyberwar act or even hacktivism. See more at: J. Matusitz, *Cyber terrorism: Postmodern State of Chaos*, "Information Security Journal: A Global Perspective"2008, no 17, p. 179–187. See also E. Molfino, *Viewpoint: Cyberterrorism: Cyber "Pearl Harbour" is Imminent*, in: *Cyberspaces and Global Affairs,* ed. S.S. Costigan, J. Perry, Farnham 2012, p. 75–82.

[7] J.S. Nye Jr., *Power in The Global Information Age*, London 2004, p. 55–58.

Richard Clarke in his work on Cyber War, for example, suggests that measuring cyber power's strength should include: a) cyber offence capabilities, b) the level of cyber dependence, and c) cyber defence capabilities. His comparison between the US, Russia, China, Iran, and North Korea places Americans as the weakest nation in that respect[8]. As such, not being free of reservations, his approach captures the main characteristics of cyberspace that rest on the correlation between the level of technological and digital advancement on the one hand and exposure of the nation to cyber threats on the other.

In that respect it has been long observed that information technologies, together with the Internet as means of modern communication, act as a mighty empowerment tools. 'Asymmetric threats' or 'power equalisers' are notions that usually apply to much weaker states, as well as non-state actors that could never otherwise match the military might of the most powerful states in an exclusively material world. In 1995 Alvin and Heidi Toffler published their seminal book, *War and Anti-War*, in which they claimed that software was changing military balances around the world. 'The cheap, low-tech platforms operated by poor, small nations can now deliver high-tech smart firepower – if the weapons themselves are equipped with smart software'[9]. This bold statement should be taken with a grain of salt. Technology itself is not likely to change power relations between nations by itself, but it certainly does add to the range of tools of both state and non-state actors equipping them with new capabilities on the one hand and opening to new threats on the other.

Stuart Starr develops a novel theory of cyber power, suggesting that it should focus on four key factors: technological advances, speed and scope of operations, control of key features, and national mobilization[10]. As cyberspace has empowered a number of entities, including terrorist groups, 'hacktivists', transnational criminals, corporations, international governmental organizations, non-governmental organizations, and nation states, a prospective cyber strategy needs to employ a broad vision and holistic approach.

One of the most elaborate analyses of cyber power to date is that of David Betz and Tim Stevens. They ascertain that cyberspace is populated with numerous actors, and it is the actors that make and shape this unique environment. 'From individual citizens to civil society organizations and commercial enterprises, from terrorists and insurgents to branches of state power (militaries, intelligence agencies, etc.) to multilateral global institutions and media conglomerates, from individual nodes to whole networks, and non-humans in the form of hardware and software too'[11]. What connects all of them is global cyberspace where everyone has their

[8] R.A. Clarke, R.K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 2010, p. 147–150.

[9] A. Toffler, H. Toffler, *War and Anti-War. Survival at the Dawn of the 21st Century,* London 1994, p. 188.

[10] S.H. Starr, *Towards an Evolving Theory of Cyberpower*, in: *The Virtual Battlefield: Perspectives on Cyber Warfare*, Ch. Czosseck, K. Geers (ed.), Amsterdam 2009, p. 48.

[11] D. Betz, T. Stevens, *Cyberspace and the State*…, p. 38.

own ends and strategies. Importantly, this mainly non-physical environment affects power understood as a relationship between actors. Essentially, cyber-power is not understood as yet another kind or form of power but as a manifestation of the same holistic power in cyberspace.

Other central notions to IR and security/strategic studies like that of deterrence, compulsion, attribution[12], ambiguous symbolism of weapons, weapons of mass destruction or even balance of power also gain new facets to established meanings, complicating the already complicated world of strategy even more. It seems justified to claim that at the very least, cyber strength introduces yet another element to the power equation, rendering all other elements more relative than ever[13].

The academic discussion regarding cyber related aspects of national and international security is developing apace. Many security scholars however look at traditional notions within the domain of state security and enrich their analysis with new elements that stem form cyber world. There seems to be therefore lack of closer scrutiny from the individual-security level of analysis. Consequently the departure point of this paper is the notion of decentralisation of state security related efforts on the one hand and empowering of the individuals within the framework of 'civilianization' of security. The case of United Kingdom and its efforts to address the cyber security threats will be used to show the shifting nature of national security policies in general and cyber security in particular.

Civilianization of cybersecurity

Security is a complex and daunting notion. As with every concept in the social sciences, it leads to many understandings and interpretations. Perhaps the most comprehensive view on security, sort of a bottom line, is that security means different things to different people in different times. From the beginning of the 21st century we have observed a definite shift in how to define security, from conceptualizing it as commodity (power related phenomenon) to the emancipation of individuals or groups thereof (actors interrelation phenomenon). In his seminal article on security and emancipation, Ken Booth argues that the latter constitutes the former: 'Emancipation, not power or order produces true security'[14].

This paper employs the concept of emancipation with reference to 'civilianization' of security. Since governments and public institutions have become increasingly inefficient in providing security to citizens, especially when one takes an individual as security 'referent', it remains for private entities and non-public bodies to fill the vacuum. In this regard, the term 'civilianization' is used as a notion relating to non-military, voluntary organisations and the business/private sector

[12] N. Tsagourias, *Cyber attacks, self-defence and the problem of attribution*, "Journal of Conflict & Security Law" 2012, no 17:2, p. 229–244.

[13] For an in-depth analysis of cyberpower and its purpose see: J.B. Sheldon, *Deciphering Cyberpower. Strategic Purpose in Peace and War*, "Strategic Studies Quarterly" 2011, Summer, p. 95–112.

[14] K. Booth, *Security and Emancipation*, "Review of International Studies" 1991, no 17: 4, p. 319.

engaged by government but acting in its own right to prevent, protect, and prepare in the context of cyber strategy[15]. In other words this is a phenomenon by which ordinary civilians are acting as providers of their own security.

Similar to the discussion around counterterrorism strategy, 'civilianization' of security seems to provide decision makers responsible for state security and citizens with a middle ground in the heated debate concerning security versus civil rights and freedoms. There is a reason to juxtapose traditional/modern political terrorism and cyber war in this context. Both are characterized by indirect, secretive, and non-proportional approaches. In both cases there is a fundamental problem with attribution (more so in cyberspace) and effective engagement with the adversary. Both can be used by non-state actors, and both primarily target civilians, terrorism through the spread of fear, and cyber attacks potentially through the destruction of critical infrastructures. Finally, terrorism and cyber war alike present the international community with fundamental challenges regarding legal regimes. How do we treat terrorists? Do the Geneva Conventions bestow on them any rights? What kind of action do we define as a cyber attack?[16] If we agree on the existence of such, does it constitute an act of aggression pertinent to war?[17] These concerns and many others render traditional concepts of (state) security in dire need for reconceptualization and subsequently the role of governments and public institutions in providing it.

Since 'civilianization' emphasizes the need to include vast parts of society into coordinated actions against perceived threats, the danger of 'suspension of normal politics' is mitigated. By engaging civilians in some aspects of cyber security, governments may not only boost a sense of burden sharing but also open themselves more to the criticism and control of the public. Enlarging the stakeholder base will in this sense bring more transparency to public policies and therefore, potentially more accountability.

'Civilianization', understood as the engagement of non-military, voluntary organisations, and the business/private sector, is a form of emancipation in the sense that K. Booth wrote about in the early 1990s. Booth asserted that 'Security means absence of threats. Emancipation is the freeing of people (as individuals and groups) from those physical and human constraints which stop them carrying out what they would freely chose to do'[18]. We cannot but notice that cyber threats clearly constitute one of those physical and by all means, human, constraints. If 'civilianization'

[15] See more in K. Sliwinski, *Counter-terrorism – a comprehensive approach. Social mobilization and 'civilianization' of security: the Case of the United Kingdom*, "European Security" 2012, p. 1-19.

[16] For an interesting discussion on cyber conflicts see: M. Schmitt, *Clasification of Cyber Conflict*, "Journal of Conflict & Security Law" 2012, no 17:2, p. 245–260.

[17] Spring of 2013 saw the publication of first of its kind approach to answer these and many more questions. See: M.N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge 2013, available from: http://issuu.com/nato_ccd_coe/docs/tallinnmanual, access: 05.2014.

[18] K. Booth, *Security and Emancipation*…, p. 319.

can give societies a sense of security through greater engagement, then we should agree to perceive it as 'freeing'. Departing from such a concept, it logically follows that 'civilianization' of security in the context of cyber security implies thinking about individuals as ultimate security referents. If this is so, then it further conduces to the notion that 'civilianization' may be conceived of as a means to achieving ultimate and relatively full security of human beings in a world where 'world order' between people is more fundamental and primordial than that of states.

Importantly, as the case of United Kingdom clearly shows, the activities under 'civilianization' are not entirely managed by the government but rather initiated and coordinated. In that sense 'civilianization' denotes a situation where civilians are engaged in the conduct of actions traditionally carried out by states and where the actual realization of the tasks and initiatives tends to shift considerably to non-official civilians in the private sphere. Paraphrasing David Garland, the aims and benefits of such initiatives are not merely the off-loading ('hiving off') of troublesome state functions, or the privatization of counter-terrorist measures. Rather along the lines of 'responsibilization' strategy in the field of crime control, 'civilianization' is to be understood as spreading new forms of 'government-at-a-distance'[19].

One should also note that 'civilianization' of security within the context of cyber security may possibly bring negative effects in the realm of fifth domain. Despite an effective response on the part of the private sector too many agents entering the field of national security presents every society with accountability gap. Moreover, the constant alertness and engagement of private stakeholders runs the risk of certain weariness among the members of society, who will grow tired of a constant state of emergency/exception and may start to disregard the need for genuine involvement.

Having ascertained that let us have a closer look at British approach to cyber security. Identification of cornerstone features of specifically British approach to cyber security will allow us to address fundamental questions concerning the relationship between the state and citizen.

Cyber threats in Britain

In Britain the awareness of cyber threats has been nourished by experts pointing to vulnerabilities of computer software-run systems present in most spheres of citizens' lives. The Director of Government and Communication Headquarters, Lain Lobban, expressed his concern on many occasions, referring to the UK's critical infrastructure and threats posed by terrorists, organized criminals, and hostile foreign governments[20]. Consequently, the latest formulation of the UK's National Security Strategy – 'A Strong Britain in an Age of Uncertainty' – reflects this trend by identifying 'Hostile attacks upon UK cyberspace by other states and large scale cyber

[19] D. Garland, *The Culture of Control,* Chicago 2001, p. 124–127.

[20] *UK infrastructure faces cyber threat, says GCHQ chief*, 12 October 2010, http://www.bbc.co.uk/news/uk-11528371, access: 05.2014.

crime' among its priority one risks[21]. That is to say, the National Security Council considered this particular risk to be the one of the highest priorities for UK national security (in the period of 2010–2015), taking account of both likelihood and impact[22]. The same document stipulates, 'Government, the private sector and citizens are under sustained cyber attack today, from both hostile states and criminals. They are stealing our intellectual property, sensitive commercial and government information, and even our identities in order to defraud individuals, organizations and the Government'[23]. Along the same lines one reads the assertion regarding cyberspace as 'woven in to the fabric' of British society. It is understood as integral to the British economy and security. The access to the Internet, the largest component of cyberspace, is therefore perceived by security experts and members of the society alike as the 'fourth utility', a right rather than a privilege[24]. In that respect the risks and threats that the United Kingdom faces online are conceptualized in five broad categories: a) dependence on information and communications technology (ICT) of the national infrastructure and government and business; b) impact of the cybercrime on the cost of business operation as well as the resilience of the trade networks; c) vulnerabilities of big international events like the Olympics, which draw numbers of criminals seeking to defraud money or cause disruption; d) the potentially devastating real-world effect of attacks in cyberspace – government, military, industrial, and economic targets seen as viable aims (this is where the example of 'Stuxnet' is usually given as self-evident case[25]; e) usage of cyberspace by terrorists to organize, communicate, and influence those vulnerable to radicalization[26].

As such, the UK national security strategy does not indicate specific responses to such conceptualized risks. This is a task for the Strategic Defence and Security Review. Let us mention at this stage that there are yet eight cross-cutting National Security Tasks as identified by the National Security Strategy, amongst which one particularly stands out as relevant to the topic at hand: work in alliances and partnerships wherever possible to generate stronger responses[27]. (The next section will exclusively refer to that point). For the time being it is interesting to take a closer look at major risks as recognized by the National Security Strategy.

[21] *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, London 2010, p. 27.

[22] Based on first ever National Security Risk Assessment (NSRA)

[23] *A Strong Britain…*, p. 29.

[24] Ibid., p. 29.

[25] In 2010, the US and Israel were behind a cyber attack, mainly against Iran – Stuxnet. According to the media, Stuxnet was just one tool used by United States as part of its cyber security strategy, code-named in the case of Iran, 'Olympic Games'. The task of the malware was to get inside Iran's main nuclear enrichment facilities at the Natanz computer system and sabotage it. Officials in the White House openly talk about the efficacy of Stuxnet in setting back the Iranian Nuclear program by roughly two years. See more at: *Obama Order Sped Up Wave of Cyberattacks Against Iran*, "The New York Times", 1 June 2012. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=3&pagewanted=2&seid=auto&smid=tw-nytimespolitics&pagewanted=all, access: 05.2014.

[26] *A Strong Britain…*, p. 29-30.

[27] Ibid., p.33.

In terms of the dependence of national infrastructure on ICT as mentioned before, one notes a developing awareness of its existence. Arguably this has become one of the defining features of modern, interconnected, and knowledge-based society and economy[28]. The UK's Government defines national infrastructure as 'those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends'[29]. According to Centre for the Protection of National Infrastructure (CPNI), the UK is facing an ongoing, persistent threat of cyber attack from other states, terrorists, and criminals operating in cyberspace[30], including e-crime relating to theft, hacking or denial of service to vital systems on the one hand and on the other, daily instances of cyber espionage carried out by governments as well as private companies. Finally, cyber terrorism presents increasing risks to national infrastructure. In Britain it is understood that not all national infrastructure is labelled as 'critical'. Only those elements of the national infrastructure that if destroyed would cause the loss or compromise of the essential services leading to severe economic or social consequences or to loss of life are labelled as such. According to official data around 80 per cent of the UK's critical infrastructure is in fact privately operated[31]. Private companies do not easily release data on their security systems, but it has been confirmed that the functioning of critical infrastructure is largely dependent on ICT[32]. Government officials are not too keen on admitting the attacks; however, back in December 2012, when pressed by the media, the UK Government reluctantly confirmed that the systems that provide the country with gas, water, and electricity supplies are 'likely to have been targeted'[33]. Admittedly the awareness of such cyber threats is on the rise, yet there is a shared belief among the major stakeholders that in fact the level of protection remains low[34]. Likewise in the case of private business. The prevailing culture is that each company, especially small businesses, are responsible for their own security and so consequently employs security approaches it sees fit. There have been reported cases where many small businesses rely simply on 'word of mouth' rather than on written security policy[35].

As regards the impact of cyber-crime on business, a recently published report from Get Safe Online indicates that more than half of the British population have

[28] P. Cornish et al., *Cyber Security and the UK's Critical National Infrastructure*, London 2011, p. 1.

[29] The national infrastructure is categorized into nine sectors: communications, emergency services, energy, financial services, food, government, health, transport, and water. See more at: Centre for the Protection of National Infrastructure http://www.cpni.gov.uk/about/cni/, access: 05.2014.

[30] http://www.cpni.gov.uk/threats/other-threats/, access: 05.2014.

[31] *Cyber Security in the UK*, London 2011, p. 1.

[32] Ibid.

[33] N. Hopkins, *Hostile states using cyberwarfare to attack UK infrastructure*, 3 December 2012, http://www.guardian.co.uk/technology/2012/dec/03/hostile-states-cyberwarfare-uk-infrastructure, access: 05.2014.

[34] Ibid. See also: *Is UK doing enough to protect itself from cyber attack*, 30 April 2013, http://www.bbc.co.uk/news/uk-22338204, access: 05.2014.

[35] *2013 Information Security Breaches Survey*, London 2013, p. 6.

been victims of cybercrime[36]. It provides alarmingly valuable data: cybercrime costs the UK on average £474 million a year. Taken from a different perspective, 19 people fall victim to cybercrime every minute. Also, three times as many Brits have been victims of online crime as offline crime in the year of 2011[37]. In 2009, it was estimated that 'some 90 per cent of high street purchases are transacted by plastic, which depends on wired and wireless communication to work. That is in addition to £50 billion of consumer purchases and sales through e-commerce that takes place wholly online'[38]. Worse still, according to the first joint government and industry report into the extent and cost of cybercrime across the UK, the overall cost to the UK economy from cyber crime is estimated at a staggering £27bn per year, with the main victim being UK businesses at a total estimated cost of £21bn[39].

These examples show the scale and the immensity of the challenge. The UK's government response is threefold. It set out to: a) reduce the risk from the UK's use of cyberspace, b) exploit the opportunities from using it, and c) improve knowledge, capabilities, and decision making. This includes creating new structures such as the Cyber Security Operations Centre (hosted by GCHQ in Cheltenham) and the Office of Cyber Security (set up in the Cabinet Office). It also envisages cofounding and supporting public and private sector joint campaigns. Get Safe Online is an example of such. It is designed to raise public awareness of online security. Sponsored by a number of stakeholders (Cabinet Office, Serious Organized Crime Agency [SOCA], Microsoft, HSBC, Cable & Wireless, Ofcom, and PayPal), it aims at cooperating with a variety of community organizations, coordinating marketing PR activities and providing comprehensive and up-to-date information, advice, and tools on Internet security. One of its latest creations is 'The Rough Guide to Online Safety', a free and easily available document that provides the public with basic information on cyber security at home and the office[40]. It applies to personal computers as well as mobile devices[41]. Should the worst-case scenario happen, it sheds light on reasonable expectations that a victim of data loss could direct at police, banks, and IT suppliers and providers.

[36] *Get Safe Online* is a joint initiative between the Government, law enforcement, leading businesses, and the public sector. It aims at providing computer users and small businesses with free, independent, user-friendly advice that will allow them to use the internet confidently, safely, and securely. See more at: http://www.getsafeonline.org/nqcontent.cfm?a_id=1, access: 05.2014.

[37] *UK Internet Security: State of the Nation. The Get Safe Online Report*, November 2011, p. 5, http://www.getsafeonline.org/media/GSOL_2011_Annual_Report.pdf, access: 12.2011.

[38] *Digital Britain: The Final Report 2009*, London 2009, p. 7.

[39] *The Cost of Cyber Crime: A Detica report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office*, London 2011, http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf, access: 05.2014.

[40] Available at: http://www.getsafeonline.org/media/GetSafeOnline_RoughGuide.pdf, access: 05.2014.

[41] According to Ofcom's *International Communications Market Report 2011*, Internet use on mobiles in the UK is one of the highest in the world and has more than doubled since 2008. See more at: http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr11/icmr/ICMR2011.pdf, access: 05.2014.

The next category of threat as envisaged by British National Security Strategy refers to potentially devastating real-world effect of attacks in cyberspace – government, military, industrial, and economic targets seen as viable aims. Before going into detail, a few words of explanation are in order. Generally speaking, most decisions makers, security experts, and increasingly societies are afraid of the looming cyber war understood as an act of physical destruction (involving kinetic force) initiated by the use of computer software. Richard Bejtlich rightly reminds us that cyber activity relating to national security could be categorized in three different stages: computer network defense (CND), computer network exploitation (CNE), and computer network attack (CNA)[42]. The first of these is usually understood as protecting digital information. The second is most often equated with espionage. The third is equated with an act of cyber war. Whereas computer network exploitation (CNE) may include penetrating computer networks to steal sensitive data such as trade secrets or defense related information, computer network attack (CAN) is a step further, so to speak. CNA may involve anything from altering through disrupting to destroying computer systems either virtually or physically. As such, it is understood that changing database records or deleting data as well as causing physical damage to computers or other equipment or inflicting any other harm is pertinent to aggression. The difference between CNE and CNA may seem obvious, but in reality there is a fine line between the two. Given the characteristics of cyberspace, any adversary that can carry out a successful act of espionage also has the capabilities of mounting a successful attack.

In Britain there has recently been much realization of this kind of threat, mostly in the context of critical infrastructure again. In mid-May 2013, the government's director of the Office of Cyber Security, James Quinault, warned that the UK 'is faced with the threat of imminent cyber sabotage, endangering not just online systems, but real-world operations'[43]. According to government officials, back in 2012 Britain was the target of up to one thousand cyber attacks every hour in a campaign to steal secrets and/or disable systems[44]. Media reported staggering amounts of information of 'hackers and foreign spies who allegedly are bombarding government departments and businesses around the clock. As well as targeting state or trade secrets, the cyber criminals and anarchists also try to disrupt infrastructure and communications, and even satellite systems'[45]. To make matters worse, it has been pointed out that since the military is so dependent on computers and information

[42] R. Bejtlich, *Don't Underestimate Cyber Spies. How Virtual Espionage can Lead to Actual Destruction*, 2 May 2013, http://www.foreignaffairs.com/articles/139357/richard-bejtlich/dont-underestimate-cyber-spies, access: 05.2014.

[43] T. Brewster, *UK Government Fears Destructive Cyber Sabotage*, 16 May 2013, http://www.techweekeurope.co.uk/news/cyber-sabotage-james-quinault-116477, access: 05.2014.

[44] T.Whitehead, *Britain is target of up to 1,000 cyber attacks every hour*, 22 October 2012, http://www.telegraph.co.uk/news/uknews/crime/9624655/Britain-is-target-of-up-to-1000-cyber-attacks-every-hour.html, access: 05.2014.

[45] Ibid.

technology, a successful CNE or CNA could render entire combat units useless[46]. According to the report by the Commons Defence Committee, such a threat is very real indeed. It is no longer just media speculation that for example satellites could quite realistically be the next target allowing the vulnerabilities of communication and transportation systems to be explored by the enemy, be it a state or non-state actor. In fact the Royal United Services Institute, one of the most established think tanks in the UK, officially warns about such threats in its numerous publications as well as seminars and conferences[47].

Finally, is the use of cyberspace by terrorists to organize, communicate, and influence those vulnerable to radicalization. On the one hand, the United Kingdom is seen by many radicals, especially Islamists, as one of the western powers to be targeted. As the major ally of the United States, the UK took part in 2003 in war against Iraq, despite much international community disagreement about the legal framework of the whole operation. On the other hand, Britain is home to a large community of Muslims, mostly of Pakistani origin. Regardless of the exact numbers, Britain has indeed one of the biggest Muslim minorities in the EU – 2.7 million in 2011 according to the United Kingdom Census 2011 held by the office for National Statistics[48]. It does not take a rocket scientist to connect the dots and pay special attention to immigration and social (mainly integration) policies. Not surprisingly, the July 2005 coordinated bombings on three underground trains were carried out by individuals holding British Passports. According to one of the latest research publications by the Centre for Social Cohesion, titled *Islamist Terrorism. The British Connections,* 60 per cent of IROs (Islamic Related Offences) carried out in the UK between 1999 and 2009 were perpetrated by individuals holding British nationality[49]. Our attention is also drawn to the relationship between international terrorism and the UK's seemingly domestic matters. Again, according to the abovementioned report, more than a quarter of those who committed IROs in Britain have Pakistani origins. Even more alarming, the majority of those had no direct link to any terrorist organization and did not attend any terrorist training. In other words, they are individuals acting in their own right on religious and ideological grounds. This presents British authorities with dire challenges, as it diminishes the efficacy of responses by central organs of the state.

[46] *Defence Committee Defence and Cyber – Security : Government Response to the Committee's Sixth Report of Session*, March 2013, p. 3.

[47] Royal United Services Institute (RUSI) has established Cyber Space and Cyber Security as one of its major research areas. It includes four major issues: cyber warfare and the legal framework for responding to cyber crime, the role of cyberspace in military operations, the role of cyberspace in the national security of the UK and legal frameworks that govern the use of offensive cyber capabilities. See more at: http://www.rusi.org/research/programmes/ref:P4CE28D3E190C2/.

[48] See more at: http://www.ons.gov.uk/ons/rel/census/2011-census/detailed-characteristics-for-local-authorities-in-england-and-wales/sty-religion.html, access: 05.2014.

[49] *Islamist Terrorism. The British Connections*, http://conservativehome.blogs.com/files/1278089320islamist_terrorism_preview.pdf, access: 05.2014.

The International Centre for the Study of Radicalization and Political Violence, a think tank based in London, published an interesting report back in 2009 that fits perfectly into the discussion. It identifies the Internet as a particularly useful tool for extremists and terrorists in their quest for radicalization and recruitment. In particular, three aspects of the Internet are accounted for as especially relevant: a) the Internet can be used by extremists to illustrate and reinforce ideological messages and/or narratives. Through the Internet, potential recruits can gain near-instantaneous access to visually powerful video and imagery which appears to substantiate the extremists' political claims; b) the Internet makes it easier to join and integrate into more formal organizations. It provides a comparatively risk-free way for potential recruits to find like-minded individuals and network amongst them, enabling them to reach beyond an isolated core group of conspirators; c) the Internet creates a new social environment in which otherwise unacceptable views and behaviour are normalized. Surrounded by other radicals, the Internet becomes a virtual 'echo chamber' in which the most extreme ideas and suggestions receive the most encouragement and support[50].

In the case of the 7th July 2005 London bombings, government reports confirmed that although the four perpetrators were not linked to al-Qaeda, they obtained at least some of the information and materials they needed for the attack from the Internet[51]. Consequently the Home Affairs Committee of the British parliament considered the Internet to play the major role in the radicalization of terrorists and has called on the government to pressure Internet Service Providers in Britain and abroad to censor online speech[52].

Public goods in private hands – the path towards 'civilianization' of cyber security?

This part sets out to sketch the general picture regarding the nature of cyber security realm in terms of its ownership and usage. Numerous examples show the extent to which the phenomenon of 'civilianization' of cyber security is taking place on British grounds.

As mentioned before, in Britain as elsewhere, the infrastructure of Internet systems is predominantly in the hands of the private sector. Therefore governments find themselves compelled to contract a very large number of civilians employed in

[50] *Countering Online Radicalization. A Strategy for Action*, London 2009, p. 11. Available at: http://icsr.info/wp-content/uploads/2012/10/1236768491ICSROnlineRadicalisationReport.pdf, access 05.2014.

[51] *Report of the Official Account of the Bombings in London on 7th July 2005*, London 2006, p. 25. http://www.official-documents.gov.uk/document/hc0506/hc10/1087/1087.pdf, access: 05.2014.

[52] *Home Affairs Committee - Nineteenth Report. Roots of violent radicalization*, http://www.publications.parliament.uk/pa/cm201012/cmselect/cmhaff/1446/144602.htm, access: 05.2013. In this regard cases of Oklahoma City bomber Timothy McVeigh, Columbine High School massacre back in 1999 or Anders Breivik killing rampage of 77 people in Oslo in 2011 show how internet cab spread and reinforce radical thoughts.

private companies to work as providers of national security. The British situation is no different. 'The Cyber Security Strategy of the United Kingdom', issued in 2009, declares a strong commitment to a public/private partnership[53]. Likewise, the latest iteration of cyber security strategy from 2011 emphasizes the indiscriminate character of cyber threats and identifies the need for strong public-private partnership. 'Though the scale of the challenge requires strong national leadership, Government cannot act alone. It must recognize the limits of its competence in cyberspace. Much of the infrastructure we need to protect is owned and operated by the private sector. The expertise and innovation required to keep pace with the threat will be business-driven'[54]. It goes on to indicate the roles and responsibilities of individuals, the private sector and the government. It envisages that individual citizens have a great role to play in keeping cyberspace a safe 'place'. In particular, 'everyone, at home and at work, can help identify threats in cyberspace and report them – for example, identifying fraudulent websites'.

The Cyber Security Challenge (SSC) is one such example[55]. It is a series of national online games and competitions that test the cyber security abilities of individuals and teams from every walk of life. It is supposed to identify skilled persons that may one day become members of a future corps working within the cyber security infrastructure of the country. Amid alarming trends of decreasing employment in the IT industry in the UK, this particular initiative refers to job categories as defined by the Institute of Information Security Professionals. It embraces such posts as strategy and policy managers (cat. 1), Incident and Threat Management and Response (cat.3), Engineering, Architecture, and Design (cat. 5) and Lawyer for advice and prosecution re data protection and Internet crime (cat. 8)[56].

Among members of the consortium that stands behind the SSC, we find The Institute of Information Security Professionals, Royal Holloway University of London, the Cabinet Office of Cyber Security and Information Assurance, and the Police Central e-crime Unit[57].

The Winners of 2010 competitions won prizes, from internships with sponsors and complimentary entries to CREST (Council of Registered Ethical Security Testers)[58] and CRT (Crest Registered Tester) exams, to affiliate memberships in

[53] See more at: http://www.cabinetoffice.gov.uk/content/cyber-security, access: 05.2014. See also: *European Union Committee – Fifth Report. Protecting Europe against large-scale cyber-attacks*, http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/6802.htm, access: 05.2014.

[54] *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, London 2011, p. 22.

[55] See more at: https://cybersecuritychallenge.org.uk/, access: 05.2014.

[56] For the full list of job categories as defined by the Institute of Information Security Professionals refer to: https://cybersecuritychallenge.org.uk/jobs-survey.php, access: 05.2014.

[57] For the full list of consortium members see: https://cybersecuritychallenge.org.uk/about.php, access: 05.2014.

[58] See more at: http://www.crest-approved.org/index.html, access: 05.2014.

the IISP (Institute of Information Security Professionals)[59], and free places in conferences of the ISC (International Supercomputing Community)[60], and the ISSA (Information Systems Security Association)[61].

One of the supporters of CCS is a private company, Science Applications International Corporation (SAIC), an American entity founded in 1969[62]. As one of the providers of scientific solutions for the US military, the Department of Defense, and the intelligence community, it specializes in cyber security. With its projects it addresses complex cyber security challenges through cyber security campaigns; community outreach programs dedicated to science, technology, engineering, and mathematics (STEM); and academic initiatives designed to help the nation and inspire future generations through cyber research, innovation, and education.

As for the private sector, its responsibility is stipulated at an even greater level. By 2015 (the timeline envisaged by the 2011 strategy), private sector companies are expected to: a) protect commercially sensitive information, intellectual property and customer data; b) work in partnership with each other, Government and law enforcement agencies, sharing information and resources to transform the response to a common challenge; and c) invest and create centres of excellence to provide the cyber security skills we will need in future[63].

In June 2011, former Defence Secretary Dr Liam Fox stressed the importance of cooperation between government and business during his speech at the London Chamber of Commerce and Industry Annual Defence Dinner[64]. His words clearly emphasized the government stance: 'But I look to you to recognize the seriousness of this issue - and to work with me to improve our national security and our competitive advantage.'

The initial reaction of industry towards the UK Government Cyber Security Strategy has been positive. Especially well received was the recognition of the critical role that the sector's small and medium-sized enterprises can play[65].

Intellect's Cyber Security group could serve as an example of a well-established platform that provides a coherent voice for industry working in 'high threat' areas (including defence, national security and resilience, the protection of CNI, intelligence, and organized crime)[66]. The group provides a channel for government, industry, and the wider stakeholder community to discuss policy, strategy, and imple-

[59] See more at: https://www.instisp.org/SSLPage.aspx, access: 05.2014.

[60] See more at: http://www.isc-events.com/isc12/, access: 05.2014.

[61] See more at: https://www.issa.org/conf/?p=105, access: 05.2014.

[62] http://www.saic.com/about/history.html, access: 05.2014.

[63] *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, London 2011, p. 23.

[64] *Dr Fox tells business we must work together to combat cyber attacks*, 8 June 2011, http://www.mod.uk/DefenceInternet/DefenceNews/DefencePolicyAndBusiness/DrFoxTellsBusinessWeMustWorkTogetherToCombatCyberAttacks.htm, access: 05.2014.

[65] *UK Government Cyber Security Strategy: the industry responds*, 28 November 2011, http://www.info4security.com/story.asp?sectioncode=10&storycode=4128435, access: 05.2014.

[66] See more at: http://www.intellectuk.org/defence-and-security-members-councils-groups/5697.

mentation issues[67]. Intellect's members include key players in cyber security, and the Trade Association provided a collective voice to Government during the development of the Cyber Security Strategy. The organization boasts 800 member companies, ranging from major multinationals to SMEs, accounting for approximately 10 per cent of the UK's GDP[68]. In addition, a number of government departments and bodies participate in Intellect. They include among others: Department for Business, Innovation and Skills (BIS), Department for Work and Pensions (DWP), Intellectual Property Office (IPO) or HM Revenue & Customs (HMRC)[69].

Referring to the role of SMEs, Gordon Morrison, Director of Defence and Security at Intellect, emphasized the importance of encouraging 'cyber aware' behaviour. Good practice guidelines are to be developed by the group, many of whose members are in the frontline of the battle against cyber threats and fully committed to working in this new partnership with government to build a safe digital environment. Members of Intellect not only have access to government officials but also up-to-date industry information and inside knowledge. They have a long list of business guidance publications and offer both guidelines and discounted training courses.

In that connection the UK government published 'Cyber Security Guidance for Business' back in 2012. As a coordinated set of guidelines on tackling threats, the initiative is especially targeted at senior levels in the UK's largest companies[70]. It proposes ten critical areas, from establishment of risk management regime through malware prevention to home and mobile working practices as tangible steps allowing to decidedly reduce cyber risks[71].

Furthermore, on the 27th March 2013 the British Government launched a new initiative that perfectly fits in to the logics of 'civilianization' as envisaged in this paper. Based on a pilot scheme known as Auburn (carried out in 2012), a Cyber Security Information Sharing Partnership (CISP) has been established. Designed as the key component of the British cyber security strategy, CISP is designed to serve as a platform for sharing information on threats that private businesses face in cyberspace[72]. Initially the project has been directed at the companies within critical national infrastructure (CNI) sectors. The key element in the architecture of the CISP is the so-called 'Fusion Cell', a combination of MI5 (the British Security

[67] Intellect has close relationship with a number of Government stakeholders that includes various UK Government departments, e.g. Home Office, Foreign and Commonwealth Office, and Department for Communities and Local government. See more at: http://www.intellectuk.org/defence-and-security-stakeholders, access: 05.2014.

[68] See more at: http://www.intellectuk.org/about-intellect/who-we-are, access: 05.2014.

[69] See more at: http://www.intellectuk.org/sme-zone/sme-government-support, access: 05.2014.

[70] See more at: https://www.mi5.gov.uk/home/news/news-by-category/government/cyber-security-guidance-for-business-launched.html, access: 05.2014.

[71] See more at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73129/12-1121-10-steps-to-cyber-security-advice-sheets.pdf, access: 05.2014.

[72] See more: https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security, access: 05.2014.

Service) and GCHQ (Governments Communication Headquarters – British intelligence agency) and industry experts. The idea stems from the realization that the government itself is not able to solve cyber security risks by itself, so it is believed that the second-best solution would be to act as facilitator of cooperation between various branches of state bureaucracy and private agents[73].

In 2013 the Cabinet Office issued its report on progress to self-evaluate two years that passed since the introduction of the National Cyber Security Strategy[74]. On a declaratory level it is yet another governmental document one should take with a grain of salt. It does however mention some interesting solutions that are relevant to the topic at hand. National Computer Emergency Response Team (CERT-UK) is declared to help critical infrastructure providers and Government co-ordinate responses to cyber incidents[75]. In fact formally launched in March 2014, CERT-UK is supposed to act as information hub for government, industry, and academia. Moreover it is devised a central mechanism to coordinate the whole country cyber-security defence.

CESG (Communications-Electronics Security Group – an institution within Government Communication Headquarters) provides assistance to government departments on their own communications security. The UK National Technical Authority provides information assurance, including cryptography. As such it is responsible for identifying companies that meet CESG-CPNI quality assurance standards for dealing with cyber incidents[76]. Here again in reality, it is the private companies that provide security for both public and private actors, since under the Cyber Incident Response Scheme (initiated back in 2012) a small number of providers are identified to deliver CIR (Cyber Incident Response)[77].

The most significant development in terms of 'civilianization' of cyber security that is present on British ground sees the creation of Joint Cyber Reserve Unit (JCRU). The aim of such is conceived as a backbone of military cyber capability. As such formally part of Ministry of Defence (MOD) the unit is recruited from acting members of the military service, reservists as well as private citizens, who if admitted, will work alongside[78].

---

[73] See more: https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security, access: 05.2014.

[74] *The National Cyber Security Strategy. Our Forward Plans – December 2013*, London 2013, p. 7.

[75] GovCertUK is part of the Communications and Electronic Security Group (CESG). As such it is the Computer Emergency Response Team (CERT) for U.K. Government. It assists public sector organizations in responding to computer security incidents and provides advice to reduce the threat exposure. GovCertUK also works closely with the Centre for the Protection of National Infrastructure (CPNI), which coordinates the response activity to electronic attacks against the U.K. Critical National Infrastructure (CNI). See more at: http://www.cesg.gov.uk/policyguidance/GovCertUK/Pages/index.aspx, access: 05.2014.

[76] *CESG. The Information Security Arm of GCH*, Gloucestershire, April 2013, p. 3.

[77] See more at: http://www.cesg.gov.uk/servicecatalogue/cir/Pages/Cyber-Incident-Response.aspx, access: 05.2014.

[78] See more at: https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit, access: 05.2014.

The Limitations of British Cyber Security Strategy

According to a report issued by Chatham House in September 2011, 'It is shared by many of those interviewed, suggesting that key sectors of British society remain generally unaware, uninformed or unimpressed about the development and scope of the government's cyber security policy and strategy. These issues prompt questions about an awareness gap in public-sector outreach and partnership'[79]. The same document reads a couple of pages later: 'Given their expertise in emergency planning one might expect the emergency services to have in place the appropriate arrangements to import specific and codified best practice in cyber-related (and other) contingencies, for example drawing from guidance supplied by the UK Cabinet Office Emergency Planning College (EPC) at Easingwold. But these do not seem to have been applied for cyber security'[80]. Generally there is reluctance to share information with institutions that might be targeted, that at the same time tend to tolerate an unacceptably high level of risk[81].

These obviously indicate the weakness of the strategy associated with its relative novelty. As such, this framework currently lacks sufficient substance to permit accurate estimations of costs. As Paul Davis, the director of Europe at FireEye, states, 'As welcome as the announcement is, concrete steps need to be taken now. Initiatives coming into being in 2013 are too far in the future. The threat is real, it's happening now and it's well recognized by the agencies mentioned. We're ready to contribute: we want to get on board'[82].

Secondly, Public-Private ownership stipulated by UK cyber strategy does face an important limitation. Private companies are understandably reluctant to share certain information because of either its potential or factual economic value. Furthermore, they are primarily responsible to their shareholders whose foremost objective is economic gain. Lastly, in the case of the UK, many of the leading utilities companies are substantially owned by overseas companies, such as German E.on and French EDF (Électricité de France S.A.)[83].

With Chinese authorities allegedly acknowledging the existence of a military unit dedicated to cyber warfare activities[84], the UK finds itself investing extensively in cyber offensive capabilities[85]. Out of the total £650m assigned for cyber security

[79] P. Cornish, D. Livingstone, D. Clemente, C. Yorke, *Cyber Security and the UK's Critical National Infrastructure*. *Chatham House Report*, September 2011, p. 11.

[80] Ibid., p. 14.

[81] *UK critical systems cyber warning*, 14 September 2011, http://www.bbc.co.uk/news/technology-14917744, access: 05.2014.

[82] See more at: *UK Government Cyber Security Strategy: the industry responds*, 28 November 2011, http://www.info4security.com/story.asp?sectioncode=10&storycode=4128435, access: 05.2014.

[83] B. Grauman, *Cyber-security: The vexed question of global rules. An independent report on cyber-preparedness around the World. Security & Defence Agenda*, Brussels 2012, p. 81.

[84] *China Acknowledges Existence of Cyberwarfare Unit*, http://www.infosecisland.com/blogview/14012-China-Acknowledges-Existence-of-Cyberwarfare-Unit.html, access: 05.2014.

[85] *UK Investing Heavily in Cyber Offensive Capabilities*, 7 September 2011, http://www.infosecisland.com/blogview/16339-UK-Investing-Heavily-in-Cyber-Offensive-Capabilities.html, access: 05.2014.

(based on the Strategic Defence and Security Review of 2010), the Government Communications Headquarters, responsible for cyber attacks, got the lion's share, 90 per cent of the budget[86]. It is logical to conclude that there seems to emerge a division of labour between the government and the private sector, with the former heavily engaged in cyber offensive activities and the latter co-responsible for a cyber defensive posture.

Drawing conclusions: from digital Pearl Harbour to 'government-at-a-distance'

In recent years, government and private sector experts have been examining a number of different scenarios. One of them, often referred to as a 'digital Pearl Harbour' attack, assumes that there is a massive cyber assault on the major computer systems of a state. According to this scenario, cyber warriors would infiltrate these systems and consequently sabotage them. They could at a later stage shut down part or all of a nation's power grid and/or attack water and fuel lines. This in turn might paralyze the state, at least for some time. Such actions are likely to create complete chaos among the citizens of the state attacked. No electricity means no services of any kind, which thus undermines the security of individuals, rendering them victims to all sorts of uncontrolled and unorganized violence.

Contingency planning appears to be one of the reasonable responses, designed not as much to prevent as to mitigate the consequences of actions aimed at paralyzing or destroying vital service providers and their facilities. In Britain these vital services are grouped under Critical National Infrastructure (CNI). The Centre for the Protection of National Infrastructure (CPNI) is an interdepartmental body that advises government and appropriate non-governmental agencies, as well as sections of commerce and industry whose services and products form part of the Critical National Infrastructure[87]. It is important to note that possibly as much as 90 per cent of the UK CNI is not government owned, and a large proportion of that is under foreign ownership[88]. In this regard, CPNI informs about basic common sense security planning within a framework of business continuity planning (BCP), staff training, awareness, and relevant standards and specifications.

In terms of prevention, the task is obviously much more demanding and cannot solely rest on public bureaucracy if it is to be effective. Just as a traditional military force undergoes a substantial review of its usefulness and purpose, so do policing in general and criminology in particular. In this respect, David Garland's 'respon-

[86] See also: *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, London 2010, p. 47.

[87] See more at: http://www.cpni.gov.uk/about/context/, access: 05.2014.

[88] P. Cornish, *Domestic Security, Civil Contingencies and Resilience in the United Kingdom. A Guide to Policy*, http://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/0607ukresilience.pdf, p. 20, access: 09.2014.

sibilization' strategy offers help in comprehending the role of policing institutions in a post-modern society. Responsibilization strategy is an attempt to extend the reach of state agencies by linking them up with actors in the 'private sector' and 'the community'[89]. As he asserts, one of the characteristics of new means of crime prevention in the USA and the UK in the last two decades of the twentieth century included addressing crime in a more indirect way. Instead of engaging police, courts, and prisons, this new approach increasingly promotes actions by non-state organisations and actors. That is to say, the state alone is not and cannot be responsible for preventing and controlling crime. In this vision, the role of the state is to 'augment and support' multiple actors and informal processes. 'Responsibilization' is not to command and control but rather to persuade and align, to organise other actors, property owners, retailers, and individual citizens, to play their parts[90].

In such a context this paper invokes the idea of 'civilianization' of security with regards to cyberspace. Given the characteristics of the so-called fifth domain, especially perhaps the asymmetric character of cyber threats, it appears that the British case analysed above holds a potential answer to the fundamental problems that democratic systems face when providing security for their citizens. 'Civilianization' of security denotes a situation where non-military, voluntary organizations, and the business/private sectors engaged by government but acting in their own right, work to prevent, protect, and prepare in the context of cyber strategy. In other words, shifting the balance between the public and the private in the direction of the latter appears to be one of the viable chances that contemporary societies have when preserving their security.

For public, academic, and policy makers, 'civilianization' is therefore largely relevant and should become both a practice and an object of study, especially in terms of its limitations and possible negative ramifications for national as well as individual security.

Key words: human security, Great Britain, civilianization, cyber security

Piąta domena – bezpieczeństwo narodowe w rękach prywatnych? Ucywilnienie bezpieczeństwa cyfrowego w Zjednoczonym Królestwie

Obecnie odchodzi się od myślenia o bezpieczeństwie w kategoriach bezpieczeństwa narodowego na rzecz bezpieczeństwa indywidualnego/ społecznościowego, które to leżą u podstaw tzw. *human security*. Jednocześnie postęp technologiczny niesie ze sobą nowe wyzwania i zagrożenia dla tradycyjnie pojmowanego bezpieczeństwa narodowego (państwowego) oraz bezpieczeństwa jednostek. Niniejszy artykuł przedstawia analizę strategii bezpieczeństwa cyfrowego Wielkiej Brytanii w świetle wyżej wspomnianych zjawisk. Głównym punktem studium są tzw. „nowe zagrożenia" wynikające z platformy cyfrowej oraz specyficznie bry-

[89] D. Garland, *The Culture*..., Chicago 2001, p. 124-127.

[90] See more at: http://news.sky.com/skynews/Home/UK-News/Soca-Names-Career-Criminals-Online-So-Public-Can-Monitor-Them-And-Report-Unusual-Behaviour/Article/201006215646937?f=rss, access: 05.2014. Also: http://www.soca.gov.uk/news/239-ancillary-orders-published-to-aid-lifetime-offender-management, access: 05.2014.

tyjskie podejście do ich rozwiązania. Jednocześnie poruszona jest tematyka zdolności oraz zakresu możliwości przeciwstawienia się współczesnych państw liberalno-demokratycznych nowym wyzwaniom i zagrożeniom w świetle podstawowych swobód obywatelskich. W tym kontekście umiejscowiona jest koncepcja ucywilnienia bezpieczeństwa państwa jako potencjalnego łącznika, swego rodzaju środka zaradczego, w konflikcie pomiędzy bezpieczeństwem narodowym (państwowym) a wolnością obywateli.

Słowa kluczowe: *human security*, Wielka Brytania, ucywilnienie, bezpieczeństwo cyfrowe

Cyberespace – la sécurité nationale dans des mains privées? Prise en main par les civils de la cybersécurité au Royaume-Uni

De nos jours on cesse d'appréhender la sécurité en termes de sécurité nationale, au profit de la sécurité de l'individu / de la communauté, qui elles-mêmes sont à la base de la sécurité humaine. En même temps le progrès technologique fait apparaître de nouveaux défis et de nouvelles menaces à l'encontre de la sécurité nationale (étatique) traditionnellement définie et de celle des personnes. L'article présente une analyse de la stratégie de sécurité numérique de la Grande Bretagne à la lumière des phénomènes mentionnés ci-dessus. Le point principal de l'étude sont les „nouvelles menaces" issues de la plate-forme numérique et l'approche particulièrement britannique d'y répondre. En même temps, à la lumière des libertés citoyennes fondamentales, est soulevée la question de la capacité des États démocratiques libéraux modernes et des modalités de faire face aux nouveaux défis et aux nouvelles menaces. Dans ce contexte est présenté le concept de „prise en main par les civils" (*civilianization*) de la sécurité de l'État comme lien potentiel, voire comme remède dans le conflit entre la sécurité nationale (étatique) et la liberté des citoyens.

Mots-clés: sécurité humaine, Grande Bretagne, prise en main par les civils, cybersécurité

Пятая домена – национальная безопасность в частных руках? Огражданствление цифровой безопасности в Соединенном Королевстве

В настоящее время многие отходят от восприятия безопасности как национальной безопасности, а начинают ее воспринимать как безопасность человека / общества, которая лежит в основе так называемой human security. В то же время технический прогресс несет с собой новые вызовы и угрозы для традиционно определяемой национальной (государственной) безопасности и безопасности личностей. Данная статья представляет собой анализ стратегии цифровой безопасности в Великобритании с учетом вышеупомянутых явлений. Главным пунктом исследования являются так называемые «новые угрозы», вытекающие из цифровой платформы, и особый британский подход к их решению. Кроме того, в статье затрагивается также вопрос способности и объема возможности противостояния современных либерально-демократических государств новым вызовам и угрозам в свете основных гражданских свобод. В этом контексте лежит понятие «цивилинизации» безопасности государства как потенциального переключателя, своего рода предохранительного средства, в конфликте между национальной (государственной) безопасностью и свободой граждан.

Ключевые слова: безопасность человека, Соединенное Королевство, огражданствление, цифровая безопасность