G-SEC WORKING PAPER No.31

Cyber security in the United Kingdom: Security, Strategy, and the Rationalization of Risk

G.R. Dalziel[1]

August 2012

Abstract

In recent years the UK government has created a National Cyber Security Programme that includes a substantial amount of funding along with the creation of new organizations and the publication of an overarching Cyber Security Strategy. At the same time, research suggests both that the meaning of security has broadened to encompass a wider array of problems and that there has been a shift in the rationality of strategic thinking from a logic of threat to one of risk. This paper explores the path the UK took in its cyber security strategy and organization from an institutional perspective. We argue that the UK state's perception of cyber security can be broken into four distinct historical periods. More substantially, as the meaning of security broadens and favors risks over threats that there is a concomitant changes at the institutional level that includes the creation of new organizational forms and practices in order to rationalize the logic of risk.

[1] Research Associate, G-SEC, Keio University. E-mail: gregdl@sfc.keio.ac.jp

1. Introduction

In its most recent National Security Strategy the United Kingdom identified 'cyber security' as a "tier one risk" to its national security.[2] This was quickly followed by publishing a separate *Cyber Security Strategy* and establishing a 'National Cyber Security Programme' that included two new organizations and substantial funding of £600 million to a variety of agencies.[3] All of this would suggest the UK government is taking the idea of cyber security rather seriously; the head of MI6 said in parliamentary testimony in 2009 that, "the whole question of cyber security is shooting up everybody's agendas."[4]

This paper seeks to explore the path the United Kingdom took, principally looking at how cyber security has been conceived of through its strategy and organization. In doing so we hope to better understand the possible institutional effects of such strategic thinking. The framework we use takes as a starting point the notion that within a risk society the rationality of strategy and the meaning of security are changing. We also employ securitization theory which seeks to explain how particular issues are brought into the security domain. However, while these two separate concepts are useful starting points for understanding the how's and whys of change, securitization theory is especially inadequate for explaining what the consequences of such change — if any — is in terms of the management of security. To that end we bring in elements of the sociological and organizational strands of institutionalism to explore the effects of such changes in strategy and security.

The paper is structured as follows. We begin with an overview on strategy and the argument that the instrumental means-end rationality of strategy changes within the context of a risk society, primarily using the work of Mikkel Rasmussen; his insights into the changing nature of strategy and risk frame our

---

[2] HM Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, 2010, Cm7953

[3] It is often publicly stated as being £650 million, but £50 million of this came from within GCHQ budget.

[4] Intelligence and Security Committee, *Annual Report 2009-2010*, 2010, p.16

analysis of British strategy in the security field. We then move to an analysis of how the meaning of cyber security has evolved over a fifteen year period and identify three distinct periods of thinking about cyber security. Understanding how the meaning of cyber security has evolved within the British state enables us to better understand British strategic thinking on cyber security, the subject of the third section. Finally, we explore the organizational and institutional effects of these changes in meaning and strategy, looking at the management of cyber security in the UK. We conclude with comments and areas for future exploration.

2. Strategy, Rationality, and Change in the Institutionalization of Security

In his book *The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century*, Mikkel Vedby Rasmussen argues — using the risk society theories of Ulrich Beck and Anthony Giddens[5] — that a change in the concept of security has accompanied a fundamental change in the way that state's approach strategy. Whereas in the past a means-end instrumental rationality defined Clausewitzian strategic thinking the increasing saliency of risk in many Western societies has changed the rationality of strategy to one centered on the concept of risk. In this paper we extend Rasmussen's argument analyzing the United Kingdom's evolving strategic thinking about cyber security specifically and the cyber domain in general.

However, Rasmussen's argument is still tied to security and strategy within the framework of the use of force and the military. Yet as the meaning of security has shifted — along with the rationality of strategy — so have state security practices. In effect this entails changes both in the institutionalization of security but also that of cyber security. As such we find both new discourses and practices but also the establishment of new organizations along with an increase in new actors — state organizations, private industry, and citizens — that

[5] Ulrich Beck, *World Risk Society*, 1998, Cambridge: Polity Press;
Anthony Giddens, *Modernity and Self-Identity: Self and Society in the Late Modern Age*, 1991, Cambridge: Polity Press.

previously had nothing to do with the security field.

Strategy in the military and security domains is traditionally thought of as the linking of (military) means to (political) ends; it is "the bridge between military power and political purpose."[6] A classic formulation from B. H. Liddell Hart sees strategy as "the art of distributing and applying military means to fulfill the ends of policy."[7] Within the context of the state and security, strategic thinking and the study of strategy has largely centered, therefore, on the military and the use of force with security generally thought of as the security of the state.

Even when moved out of the military domain, the meaning of strategy revolves around the deliberate application of resources in the service of particular goals and the use of instrumental rationality to do so: "Strategy-making is typically assumed to be a deliberate, planned and purposeful activity. Conscious choice, instrumental rationality and goal-directed behaviour are supposed to underpin strategic action."[8]

Undermining the security of the state — and so what much of strategy tended to deal with — are threats. Rasmussen defines threats as "a specific danger which can be precisely identified and measured on the basis of the capabilities an enemy has to realise a hostile intent."[9] This focus on intentions and capabilities is central to the notion of threat and distinguishes it from risk, which we discuss below.

Intentions and capabilities are akin, in a sense, to means and ends. Intentions are the ends we desire (to gain or avoid) and capabilities are the means to which we achieve such ends. This typifies the rationality at work in traditional strategic thinking. While we may be able to argue about the size of a threat, or our ability to adequately gauge an opponent's intentions, a threat is finite and bounded.[10] It can be overcome and in doing so ensure one's own

---

6 Colin S. Gray, *Strategy and History: Essays on Theory and Practice*,2006,London:Routledge,p.1

7 Basil Liddell Hart, *Strategy*, London: Faber, 1967, p.321

8 Robert C.H. Chia and Robin Holt, *Strategy without Design: The Silent Efficacy of Indirect Action*, Cambridge: Cambridge University Press, 2009, p.ix

9 Mikkel Vedelby Rasmussen, *The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century,* Cambridge: Cambridge University Press, 2006, p.1

10 See Frank J. Stech, *Political and Military Intention Estimation: A Taxonometric Analysis*, Office of Naval Research, 1979; Frank J. Stech & Kenneth C. Hoffman, *Methods of Estimating*

security.

Whereas threats are largely bounded and can be analyzed through a framework of means-end rationality, risk is based around scenarios; that is, possible futures. Here we use Rasmussen's definition of risk as "a scenario followed by a policy proposal to prevent this scenario from becoming real."[11] The risk society, following Beck and Giddens, is one where risk is a central organizing principle of society and is typified by reflexivity — self-awareness and self-knowledge — and an engagement with the future. This reflexivity, of how people think about themselves and their actions, in itself creates new possible scenarios that must be dealt with. These possible futures are generally negative scenarios of future failure and create an impetus for action to avoid such scenarios being realized.[12] The rationality of risk is not just constructive but productive; that is, risk not only constructs problems but also produces calls to action to avoid such problems. Filippa Lentzos writes that moving from threat to risk entails both an engagement with possible futures, but also that these possible futures create an impetus for action:

> "Once threat is transformed into risk, those to whom this discourse is addressed can no longer submit themselves with hope or resignation to a future that will come as it may. They must act, for the future is something for which they now have responsibility." [13]

This engagement with the future, then, creates a kind of 'action bias' that often typifies government in the face of security threats. The sociologist Robert Wuthnow argues that the U.S. government has institutionalized crises;[14] in the UK, however, what we see is in fact an institutionalization of risk. This need to

---

Strategic Intentions, Office of Naval Research, 1982; Bertam F. Malle et al. (eds.)*Intentions and Intentionality: Foundations of Social Cognition*, Cambridge, MA: MIT Press, 2004; G.R. Dalziel, "Assessing the terrorist threat to the food supply: food defence, threat assessments, and the problem of vulnerability, "*International Journal of Food Safety, Nutrition and Public Health*, 4(1), 2011, pp.12-28

11 Rasmussen, *The Risk Society at* War, p.2

12 G.R. Dalziel, "Assessing the terrorist threat to the food supply: food defence, threat assessments, and the problem of vulnerability."

13 Filippa Lentzos, "Rationality, Risk and Response: A Research Agenda for Biosecurity, *BioSocieties*, 1, 2006, pp.453-464, p.461

14 Robert Wuthnow, *Be Very Afraid: The Cultural Response to Terror, Pandemics, Environmental Devastation, Nuclear Annihilation, and Other Threats*, Oxford: Oxford University Press, 2010, pp. 211-213

act, however, is not done to defeat or deter a threat but to ensure a negative future is avoided. The fact that a scenario has not occurred does not mean it will not occur in the future. While threats are well-bounded problems, the only boundaries on the future are our imaginations. As such, strategy become less about threats and more about risk, which cannot be defeated or deterred but can only be managed.[15] Indeed, in the UK's *Strategic Defence and Security Review* they write that one of the main functions of the document is to explain "how we will manage risk."[16]

Generating possible futures therefore becomes an important organizational function of government; in the UK it is often called 'horizon scanning'.[17] Existing organizations create new practices to engage in this or new organizations are established that specialize in this function. Beyond this finds both the professionalization of future-work along with attempts at standardization, training, academic qualifications, and so on. While previously this sort of work was confined to intelligence organizations or in some units of private industry[18] today it is a proliferating and profitable work.

Managing risk and engagement with the future, then, are two of the key practices arising out of this risk rationality. The third that Rasmussen identifies — and which we touch upon briefly in this paper — is what he calls the "boomerang effect."[19] This is another way of looking at the effects of the reflexivity typical of the risk society. Reflexivity essentially means that there is an awareness, a knowledge, that society itself — and one's own actions — create new vulnerabilities and so new risks that must be managed. Many identify the literature on globalization in this manner wherein globalization is perceived as

---

15 Rasmussen, *The Risk Society at War*

16 H.M. Government, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, 2010, Cm7948, p.19

17 In the UK, for example, there are: Foresight Horizon Scanning Centre (BIS), Horizon Scanning & Futures Team (Defra), Horizon Scanning and Response Team (Cabinet), DSTL Horizon Scanning Centre (MoD). For more see: Beat Habegger, "Horizon Scanning in Government: Concept, Country Experiences, and Models for Switzerland, *Center for Security Studies* (Working Paper), 2009

18 The best known example is Peter Schwartz and the use of scenario planning at Royal Dutch Shell. See also: Dan Gardner, *Future Babble: Why Expert Predictions are Next to Worthless, and You Can Do Better*," New York: Dutton, 2011; David Orrell, *The Future of Everything: The Science of Prediction*, New York: Perseus, 2007; Philip E. Tetlock, *Expert Political Judgment: How Good is it? How Can We Know?*, Princeton, NJ: Princeton University Press, 2005.

both increasing benefits and opportunity (e.g. economic, flow of goods and people) while at the same being a source of risk (e.g. transnational crime, pandemics, terrorism). The cyber domain is seen in much the same fashion, being both a source of benefit but also a source of risk that must be managed. This tension is explored throughout the paper.

Bureaucracies often enact and maintain boundaries around particular problems; we rely on these classifications, or distinctions, to maintain coherence of our environment; such boundaries constitute the institutional logic of the field in which they operate and are consequential both in terms of what role they play but also what range of practices they engage in.[20] Risk, however, is a boundary-spanning phenomenon, problematic and rather unnerving for bureaucracies because risk essentially breaks down boundaries. In blurring boundaries it widens the number of actors needed to manage risk — which crosses domains — and increases governance challenges such as control and coordination across organizational boundaries. As such one finds a rise in concepts like 'whole-of-government' policy and strategy — of which the *Cyber Security Strategy* is one. Included in this are organizations whose main function is simply to manage these cross-organizational responses to risk or to rationalize policies in order that differing organizations — with different functions, outlooks, and cultures — can cooperate and appear to manage risk in a unified fashion. In addition, we find a growing number of units and organizations to manage security in the private sector either through public-private partnerships, liaison work, the setting of standards, and so on.

This can be extended to the level of the individual citizen, where strategic communication campaigns are enacted in an attempt to change behaviors and perceptions. In their attempts to change behaviors the state attempts to

---

[19] Rasmussen, *The Risk Society at War*, p.39

[20] See Michèle Lamont, *Money, Morals, and Manners: The Culture of the French and the American Upper-Middle Class*, Chicago: University of Chicago Press, 1992; Michèle Lamont & Marcel Fournier (eds.), *Cultivating Differences: Symbolic Boundaries and the Making of Inequality*, Chicago: University of Chicago Press, 1992; John W. Mohr & Vincent Duquenne, "The Duality of Culture and Preactice: Poverty Relief in New York City, 1888-1917", *Theory and Society*, 26(2/3), 1997, pp.305-56; John W. Mohr, "Measuring Meaning Structures," *Annual Review of Sociology*, 24, 1998, pp.345-370; John W. Mohr & Helene K. Lee, "From Affirmative Action to Outreach: Discourse Shifts at the University of California," *Poetics*, 2000, 28(1), pp.47-71.

outsource some of the management of risk to the individual, which marks a change from the Cold War era where both the main locus and provider of security is the state. However, while some of the management of risk is outsourced to the individual, the main provider is still the state.

In this paper, then, we combine the insights from this concept of strategic risk rationality within an institutional framework in order to analyze how the UK got to where it is today with cyber security seen as a prime threat to national security, an overarching domain-crossing strategic framework has been constructed, new organizations have been created, along with substantial funding to pre-existing organizations.

To understand this path a little better we therefore begin with analyzing the shifting discourse regarding risk and security within the cyber domain; after understanding the changing meaning of cyber security we then look at the variety of strategies the United Kingdom has engaged in to manage cyber risk. Finally, we look at the new organizations and practices that have emerged from these two factors.

3. Finding Cyber Security in the United Kingdom

To examine why the U.K. has crafted its strategy and its approaches to cyber security in the manner they have, it's important we have an adequate understanding of what cyber security means to the state. By creating definitions and categories we create boundaries that are both mental and practical. How, then, does the government define cyber security and has this changed over the years? To that end we utilize a method called 'discourse tracing' that essentially involves tracking conceptual change over time.[21] We analyzed a select number of publicly available strategies and annual reports of various organizations (government agencies and parliamentary oversight committees) and public speeches by policymakers over a fifteen year period.

In doing so we can begin to map out how the meaning of cyber security has changed over time, along with the concepts of risk, threat, and security. Looking

[21] David L. Altheide, "Tracking Discourse and Qualitative Document Analysis," *Poetics*, 27, 2000, 287-299;

at these changes helps us understand the broader institutional changes of security at work in the United Kingdom.

These changes can be broken down into roughly three distinct periods. The first, beginning in the mid-1990s is marked by a focus on the concepts of *information warfare* along with *cyber crime*. The second, at the beginning of the 2000s sees a shift away from information warfare towards what was called *information assurance*; the category of cyber crime persists during this period. The final period, beginning around 2008 is where we find the prevalence of *cyber security.* These shifts in meaning mark changes within strategic thinking about security and risk within the cyber. More consequentially, however, is that for much of the first two periods, malicious actions within or via the cyber domain were thought of as criminal in nature and not as security threats.

Initially, threats within and via the cyber domain were to the state and to its information systems. The focus on information warfare reflects the manner in which military organizations thought about how to exploit the cyber domain within the context of the use of force. The cyber domain was seen as a tool which could be used either to influence perceptions and behaviors or impinge the sensemaking activities of an opponent. Threats to one's own information systems were largely seen within the context of state-to-state interactions.

The shift to information assurance moves us out of the military domain and reflects the growing idea that the broad use of and reliance upon the cyber domain was becoming a risk in itself. This in itself reflects an awareness of the 'boomerang' effect of the risk society and a shift towards the risk rationality that typifies strategy today. Indeed, the risk arising from a reliance on the cyber domain is exemplified by the worries over the 'Millennium Bug' during the mid-to-late 1990s:

> "The alarm over the Millennium Bug has vividly demonstrated how dependent our whole society now is on computer systems. Their security is vital to our lives, and a proper awareness of the opportunities and risks of 'information warfare' is essential. Some recent reports of individual hackers intruding into major defence installations may seem harmless incidents. Pursued on a systematic basis, and with hostile intent, they

could have devastating impact." [22]

Information assurance refers to the security of data and the systems in which data is held either from malicious actors or accidental loss or damage. In contrast to the rather vague nature in which cyber security is defined — more on which later in the paper — information assurance is concretely defined in many places.[23] The locus of security here is still largely the state and its data.

Common to both these first two periods is that outside of the state's military, intelligence, and security functions was that much of the cyber threats were characterized as crime with a concomitant government response. In fact, the first cyber crime unit was set up in 1985 within the Metropolitan Police's Fraud Squad, even before the emergence of the concept of information warfare.[24]

Cyber crime, or e-crime as it is often termed, is operationally defined in the UK but there still remains no legal definition.[25] The Home Office "believes that actions should be legal or illegal according to their merits, rather than the medium used, so that what is illegal offline should be illegal online."[26]

A study entitled *Project Trawler* commissioned by the National Criminal Intelligence Service (NCIS) [later merged into the Serious Organised Crime Agency (SOCA)] defined cyber crime in 1999 as "an offence in which a computer network is directly and significantly instrumental in the commission of the crime. Computer interconnectivity is the essential characteristic." [27] Much of the activities which the government defines as malicious in connection with the cyber domain — hacking, fraud, theft of data — are viewed as acts necessitating criminal penalties and a policing response, not as threats to security.

As we move into the cyber security era what is notable is that nowhere in

---

[22] Intelligence & Security Committee, *Annual Report1997-1998*, 1998, p.vii

[23] Cabinet Office, *A National Information Assurance Strategy*, 2007; Home Office, *Cyber Crime Strategy*, 2010; Cabinet Office, *HMG Security Policy Framework*, 2011

[24] Peter Sommer, "The Future for the Policing of Cybercrime," Computer Fraud & Security, 2004, Issue 1, pp.8-12, p.8

[25] House of Lords Science and Technology Committee, *Personal Internet Security Report*, 2006-7, 2007, p.64

[26] Home Office, *Cyber Crime Strategy*, 2010, Cm7842

[27] National Criminal Intelligence Service (NCIS),*Project Trawler: Crime on the Information Highways*,1999.Available online at: http://www.fipr.org/rip/Project Trawler.htm [Accessed: 01/31/12]

either the original or updated *Cyber Security Strategy* is 'cyber security' actually defined. In fact, we could not find in any government publication or parliamentary testimony any sort of 'official' definition of cyber security. We may, however, gain a sense tangentially of its meaning through discourse tracing, but this utilization of strategic ambiguity by the UK government is in itself worth noting. [28]

What is clearly defined in the strategy is the 'cyber domain' which is defined as "all forms of network, digital activities; this includes the content of and actions conducted through digital networks."[29] As such, one would suspect that anything that impinges upon or disrupts any kind of 'digital activities' or digital content would be affecting the security of the cyber domain.

This definition of the cyber domain therefore brings in things like intellectual property into the security domain. It also means, however, that it is not merely the cyber domain that is threatened here but rather the cyber domain is itself a source of threat that must be managed. The security of the state, the private sector, and individuals are threatened both within the cyber domain and via the cyber domain. The cyber domain is that which must be secured and that which must be secured against. This is essentially a conflation of means and end — typical, Rasmussen argues, of strategic risk rationality — and in such a situation one cannot defeat or deter threats but can only manage risks.

Some might argue that such a situation where there is a shift in moving malicious actions in the cyber domain from crime to security is an example of securitization at work. Securitization theory looks at how political actors utilize speech acts to define certain things as belonging to the security domain, thereby elevating it above 'normal' politics and political responses.[30] However, while securitization theory is, we would argue, useful as a sensitizing device, it is too limited an approach. The focus on speech acts in essence limits analysis largely

---

[28] See: E.M. Eisenberg. (1984). "Ambiguity as Strategy in Organizational Communication," *Communication Monographs*, 51, 227-242; Bud Goodall, Angela Tretheway, Kelly McDonald, "Strategic Ambiguity, Communication, and Public Diplomacy in an Uncertain World: Principles and Practices", Working Paper #0604, Consortium for Strategic Communication, Arizona State University

[29] Cabinet Office, Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space, 2009, Cm7642, p.8

[30] Barry Buzan, Old Waever, Jaap de Wilde, *Security: A New Framework for Analysis*, 1998,

to discourse, but it fails to look at the rationalization of security and whether changes in discourse lead to changes in organizational practice and institutionalization.

Analyzing the strategic thinking at work along with security practices — instead of solely the rhetoric used to distinguish normal politics from security — we find that securitization theory cannot tell us much about what happens after something is securitized. Merely telling us something is now 'securitized' and the discursive strategies used to achieve such a move tells us little about whether it is consequential for how security is then managed and whether this also entails changes in the institutionalization of security.

Rasmussen demonstrates how a focus on the management of risk is changing military doctrines and practices that in fact incorporate those of the police and crime reduction. We find similar patterns of strategic thinking within cyber security with the incorporation of the rationality of crime reduction into the security sphere. However, while there is a shift in doctrines and practices, the move from crime to security does appear to be consequential in the management of risk, but securitization cannot adequately explain this shift.

4. Strategizing Cyber Security in the United Kingdom

For the UK government the cyber domain is both means and end, a source of benefit and of insecurity. The vision, or positive scenario, the UK government outlines in the *Cyber Security Strategy* highlights this risk rationality:

> "Citizens, business and government can enjoy the full benefits of a safe, secure and resilient cyber space: working together, at home and overseas, to understand and address the risks, to reduce the benefits to criminals and terrorists, and to seize opportunities in cyber space to enhance the UK's overall security and resilience."[31]

This understanding of the cyber domain remains remarkably consistent. Former Home Secretary Jack Straw, upon announcing the creation in 2001 of a

---

Boulder, CO: Lynne Rienner

[31] Cabinet Office, Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space, 2009, Cm7642, p.3)

National Hi Tech Crime Unit (NHTCU):

> "The Government is committed to action against hi-tech crime in line with our objective of making the UK the best and safest place in the world to conduct and engage in e-commerce. Modern technologies such as the Internet offer up huge legitimate benefits, but also powerful opportunities for criminals, from those involved in financial fraud to the unlawful activities of paedophiles. The significant cash injection I am announcing today will boost the police service's capability to investigate crime committed through computers, including paedophilia, fraud, extortion and hacking."[32]

While this displays elements of risk rationality that typifies current strategic thinking — note the concurrent benefits and threats from the internet — what is most significant about this is that much of the more public aspects of cyber security such as hacking and fraud are thought of as 'crime' at this point in time, not 'security.' The objectives, or scenario, which the UK government is hoping to reach — "the best and safest place in the world to conduct and engage in e-commerce" — is not too far away from that of the *Cyber Security Strategy*. Yet while the 'good' future remains the same, the risks in terms of negative futures keep expanding alongside the meaning of security. These changed meanings are constitutive of a broadening of the security field, especially in terms of actors involved, something we explore later in the next section.

The *Cyber Security Strategy*, first published in 2009 and updated in 2011, outlines three main sources of cyber risk: criminals (fraud, theft); states (espionage, use of cyber domain to disrupt infrastructure); and terrorists (communication, propaganda, and fund-raising).

The primary, ongoing and actually existing threat (versus possible scenarios) is identified as cyber crime.[33] For the security services, however, their main concern is with states engaged in espionage. What is significant about these two real, ongoing, and actually existing threats is that before the *Cyber*

---

[32] Home Office Press Release, New Hi-Tech Crime Investigators In £25million Boost to Combat Cybercrime, 13 November 2000.
Available online at http://www.cyber-rights.org/documents/hi-tech.htm. Accessed: 01/22/12.

[33] Intelligence and Security Committee, *Annual Report 2010-2011*, 2011, p.53; Cabinet Office, *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space*, 2009, Cm7624; Cabinet Office, *The UK Cyber Security Strategy: Protecting and*

Security Strategy there were (and are) actually existing strategies that have been published outlining how these risks would be managed. For cyber crime there have been a number of different strategies published,[34] while theft of information (espionage) is covered in a variety of information assurance strategies and doctrines.[35]

Indeed, a *National Information Assurance Strategy* (NIAS) was first published in 2003 and updated in 2007, just two years before the publication of the *Cyber Security Strategy.* Given the focus on hacking, on the theft or loss of data, and the risk emanating from a reliance on information systems, one would think that the NIAS would be an influential component of the *Cyber Security Strategy* yet it appears to be rather downplayed in this new strategy.

The publication of the NIAS saw the creation of a 'Wider IA Centre' (WIAC) comprised of three organizations: (1) Central Sponsor for Information Assurance (CSIA), located in the Cabinet Office (which published the NIAS); (2) Communications-Electronics Security Group (CESG) located in GCHQ and which is mainly focused on government information systems and threat to those systems; and (3) Centre for the Protection of National Infrastructure (CPNI), located in the Home Office, and focused on liaising with and providing information about threats to private industry systems. In addition, this strategy outlined roles for the Department for Business, Enterprise and Regulatory Reform (BERR) [renamed the UK Department for Business, Innovation and Skills (BIS) in 2009], the Home Office and the e-crime unit of SOCA.

While the NIAS is downplayed within the framework of the *Cyber Security Strategy* there are similarities. Both emanated from the Cabinet Office, involved attempts at coordinating multiple government agencies, liaisons with the private sector and the involvement of traditionally non-security organizations.

The difference between the two, however, is that 'cyber security' entails a

---

Promoting the UK in a Digital World, 2011.

34 Association of Chief Police Officer of England, Wales & Northern Ireland (ACPO), *ACPO e-Crime Strategy Version 1.0*, 2009; Home Office, *Cyber Crime Strategy*, Cm7842, 2010

35 Central Sponsor for Information Assurance (Cabinet Office), *A National Information Assurance Strategy*, 2007; Cabinet Office and CESG, *HMG Information Assurance Maturity Model and Assessment Framework* (Vol. 4.0), 2010; Cabinet Office, *HMG Security Policy*

far more expansive meaning of risk and security. This enlarges the security field and encompasses far more negative futures than those of information assurance. In addition, it also involves a widening the sphere of influence (in theory) for the Cabinet Office and the impetus for more control and coordination.

In such a situation threats and risk are not necessarily emanating from 'out there' (i.e. from an opponent) but can be the result of one's own efforts — the boomerang effect. This is seen in a non-security strategy — *Digital Britain* — produced by the UK government in 2009 that outlines the government's strategy for harnessing the economic impact of the internet. This included: (1) ensuring UK networks are perceived as safe and reliable; (2) protection of IP rights; (3) increase the volume of business online; and (4) increase online public service transactions and interactions to bring about "efficiencies and cost savings."[36]

Moving towards these positive futures, however, brings about the possibility of negative scenarios. Increasing the perception of safe and reliable networks requires both technical doctrines but also strategic communication campaigns that attempt to shape perceptions and behaviors; protection of IP rights necessitates legislation, monitoring, and enforcement; finally, increasing the volume of transactions online — whether for private business or public service — increases the number of potential vulnerabilities and risks. The more the UK government moves online, the more risk the UK government (and its citizens) is thought to be exposed to; hence the need for new organizations, new strategies, and new rounds of funding. Indeed, this self-induced vulnerability is outlined explicitly in the 2010 *Cyber Crime Strategy*:

> "As part of improving the efficiency of Government services, there is a drive towards better and more convenient provision of services in respect of a number of the Government's tax regimes, such as the provision of tax credits, VAT and income tax returns online. These improvements are potentially at risk from cyber criminals seeking to defraud public services or falsely obtain credentials, and we need to ensure that such services are protected from criminal exploitation."[37]

Framework, 2011

[36] Department for Culture, Media and Sport and Department for Business, Innovation & Skills, *Digital Britain: Final Report*, 2009, Cm7650; Cabinet Office, *Cyber Security Strategy of the United Kingdom*, 2009.

[37] Home Office, *Cyber Crime Strategy*, 2010, p.6

The prevalence and proliferation of strategies — a feature, Rasmussen, argues, of a risk society and something worthy of a study in its own right — highlights the reflexive nature of rationality at work within the UK government. Robert C.H. Chia and Robin Holt, in their study of organizational strategy, write that an increase in thinking about risk — something seen in both the strategies and practices of cyber security specifically and security governance in general in the UK — does not increase control as is commonly thought. Instead it merely creates more risk, and more uncertainty.[38]

The very things, then, that benefits the UK are also seen as its main source of risk. The more one operates in that domain, the more risk one potentially exposes oneself to.

Boundaries become blurry in a risk society. Not only is there no clear delineation between ends and means but the boundaries between security and non-security become increasingly undefined. Having discrete boundaries help people maintain a sense of coherence over their environment and a lack or changes in boundaries can be unsettling for people and for organizations.[39] As such, the amount of actors within the security field increases. This brings about not only new organizations but also organizational practices to coordinate and control such an enlarged field. In this next section, we highlight some of the organizations at work in the UK cyber security field.

5. Organizing Cyber Security in the United Kingdom

The *Cyber Security Strategy* designated the Cabinet Office as lead organization for cyber security efforts in the UK. This was rather fortuitous as they themselves published the strategy. To put this strategy into action, a National Cyber Security Programme (NCSP) was established alongside £600 million in new funding: 56% percent of this goes to the three security and intelligence services, with the Ministry of Defence (MoD) getting the next largest

---

[38] Chia and Holt, *Strategy without Design*, p.44

[39] Eviatar Zerubavel, *The Fine Line: Making Distinctions in Everyday Life*, Chicago: University of Chicago Press, 1991

chunk at 15%, followed by the Home Office with 11% and the Office of the Government Chief Information Office (OGCIO) getting 10%.

Two new units within the Cabinet Office were also established, one of them to manage and coordinate the NCSP. This unit, the Office of Cyber Security (OCS) sits within the National Security Secretariat and was recently renamed the Office of Cyber Security and Information Assurance (OCSIA). Alongside managing and coordinating the NCSP (including managing the overall budget) it appears much of OCSIA's work involves the rationalizations of cyber security in the UK, with the *Cyber Security Strategy* stating that its main task is to "identify gaps in the existing doctrinal, policy, legal and regulatory frameworks."[40] This sort of work is necessary when one is attempting to rationalize cross-domain, boundary-spanning risk. Strategy is often an attempt by organizations to create some coherence out of their environment;[41] one of the OCSIA's main goals is said to be "providing a joined-up and coherent strategic and policy lead for cyber security and Information Assurance across government."[42] A similar organization appears to be located within the Ministry of Defence called the "Cyber Security Policy Team" (CSPT), formed "to develop [a] unified and integrated response to [the] threat of cyber attack."[43]

The second new unit formed, the Cyber Security Operations Centre (CSOC), while organizationally situated within the Cabinet Office is actually located at GCHQ. Its remit is to "monitor developments in cyber space… analyse trends, and to improve technical coordination to cyber incidents."[44] It's unclear, however, how much duplication is involved in CSOC's work. The first *Cyber Security Strategy* identified three priorities of CSOC were to: (1) "actively monitor the health of cyber space and co-ordinate incident response"; (2) "enable better understanding of attacks against networks and users"; and (3) "provide better advice and information about the risks to business and the public."[45] In the case of coordinating incident response, for example, it is not clear how CSOC

---

[40] Cabinet Office, Cyber Security Strategy of the United Kingdom, 2009, p.18
[41] Chia and Holt, *Strategy without Design*
[42] Intelligence and Security Committee, *Annual Report 2010-2011*, 2011, p.56
[43] Tristan Kelly, "Combating Cyber Attacks", *Defence News*, May 2011, p.11
[44] Cabinet Office, *Cyber Security Strategy of the United Kingdom*, 2009, p.17
[45] Ibid., p.5

is meant to interact with the main cyber response teams: GovCertUK, CSIRTUK (CPNI), and MODCERT (MoD). While in terms of the third priority, it appears to directly conflict with the remit of the Centre for Protection of National Infrastructure (CPNI) and the Cyber Security Team located in BIS. CPNI is responsible for delivering advice on security, risk, and vulnerabilities to the private industry that control critical national infrastructure.

Ministerial responsibility for cyber security also rests in the Cabinet. However, this ministerial responsibility was not always the case. Initially, while OSC/OSCIA and CSOC (both located within the Cabinet) were supposed to lead the NCSP, ministerial responsibility lay with the Minister for Security, located in the Home Office. This division of responsibility and manpower was a concern for the Intelligence and Security Committee (a parliamentary oversight committee) along with then-Minister for Security Baroness Neville-Jones who told the Committee that "you are pointing to a formal loophole in the system, and I don't argue with you that that may exist."[46] In May 2011, responsibility transferred to the Minister for Cabinet.

What is peculiar about this situation is that the Minister for Cabinet was responsible for the *National Information Assurance Strategy* (NIAS). It is not entirely clear if the Minister for Cabinet retained responsibility for Information Assurance under the *Cyber Security Strategy*. This and the 'formal loophole' to which Baroness Neville-Jones refers, however, appears to reflect the fact that, initially at least, cyber security was understood more within the framework of crime and criminal acts (for which the Home Office has some jurisdiction) rather than security writ-large. It also reflects the division between, on the one hand, cyber crime and, on the other hand, information assurance and the attempt at the *Cyber Security Strategy* to rationalize the two areas within a coherent framework.

The Intelligence and Security Committee's *Annual Report* 2010-11 writes that there are eighteen government agencies involved in cyber security.[47] The number of agencies for the committee was apparently a problem as it brought about worries of wasted resources through duplication of effort.

---

[46] Intelligence and Security Committee, *Annual Report 2010-2011*, p.56

The amount of agencies and organizations involved, however, appears to be a gross undercount. If one includes the number of agencies involved in cyber crime (which is part of cyber security) the number goes up. The number goes up even further if one includes information assurance activities (which are part of cyber security) as a previous report found over thirty different agencies involved in this particular area. Our own research using open sources found at least forty and while numerical differences may be due to conceptual differences it is not clear if the government has a complete awareness of the breadth and depth of organizations working within the broad area of cyber security. While it is not clear if this lack of coordination is in itself a negative, there is clearly a drive and desire on the part of certain parts of the government — the Cabinet Office, oversight committees — to rationalize the coordination of these various elements of cyber security governance.

As we noted earlier, the expanding meaning of security and the boundary-spanning nature of risk is enlarging the number of actors within the security field, not only creating new organizations like the OCSIA and CSOC, but also bringing in organizations that previously had nothing to do with security. For example, while BIS is the lead organization for IP protection, the Department for Culture, Media and Sport is in charge of "online copyright protection in relation to the 2012 Olympics."[48] Both now fall within the cyber security domain.

Within the Department of Health, the Medicines and Healthcare Products Regulatory Agency (MHRA) now must deal with online fraud in relation to medicines and medical products.[49] Meanwhile, the Department of Energy and Climate Change (DECC), in the drive to develop alternative energy supplies and smart grid technology standards is having to implement cyber security risk and threat assessments both in terms of scenarios of disruption to infrastructure but also in the more mundane aspects of "fraudulent transactions for financial gain, such as prepayment fraud" using the cyber domain.[50]

---

47 Intelligence and Security Committee, *Annual Report 2010-2011*, 2011, Cm8114, p.55

48 Home Office, *Cyber Crime Strategy*, Cm7842, 2010, p.22

49 Home Office, *Cyber Crime Strategy*, Cm7842, 2010, p.24

50 Department of Energy & Climate Change, "Smart Metering Implementation Programme",

The extension of the locus of security, then, is not only shifted to private industry but all the way down to the individual — albeit with the state remaining the ultimate arbiter of security or manager of risk. This outsourcing of risk management to individual citizens in itself creates new organizations and new practices (or, perhaps, an increase in very old practices by new actors). The best example of this is the proliferation of 'strategic communication' campaigns often described as a means of 'raising awareness' or as 'outreach' to inculcate or influence changed behaviors within citizens. This is not only because security has shifted to the individual but because in a risk society, risk extends down to the individual and it is also the actions of the individual themselves that opens the door to risk.

For cyber security this includes a number of campaign to make sure people engage in 'safer' (or 'less risky') practices online to reduce their vulnerability to fraud. There are four main campaigns associated with the NCSP: (1) Get Safe Online; (2) Think U Know; (3) Click Clever, Click Safe; and (4) Cyber Security Challenge. The first three are about reducing the risk that people's actions might make them susceptible to the risk of either suffering from fraud or becoming involved in child pornography.

The final effort, the Cyber Security Challenge (CSC), is designed to attract more people to the profession of cyber security. It is interesting in the manner in which it highlights the reflexive nature of risk or the 'boomerang effect' as Rasmussen terms it. The CSC, however, is of a measure more different than the boomerang effect. While, for example, the cyber domain is conceived of as both a source of opportunity the growing dependence on it is seen as vulnerability. This is, in fact, the entire logic of the cyber security. What the CSC does, though, is to take this boomerang effect, this reflexive risk, and monetize it. This rationalization of risk is seen in that the entire point of the CSC is to attract more people to careers in cyber security. As more people engage with a digital economy, more people are needed to manage cyber risk.

The *Cyber Security Strategy* also tasked or identified a number of organizations with building up and promoting an indigenous cyber security

---

2011, p.47

industry; as such this necessitates liaison work, advisory bodies, and and funding with both private enterprises and academia. This includes not only the Cyber Security Team at BIS, but also the UK Trade & Investment department identified in the *Cyber Security Strategy* to:

> "Work with the security sector's trade associations to make sure that this increasing domestic strength is leveraged to help UK firms sell abroad. We will turn the threat into opportunity and make strong cyber security a positive for all UK businesses and part of the UK's competitive advantage."[51]

6. Conclusion

In analyzing Britain's *Cyber Security Strategy* we find an ambitious attempt to craft a coherent strategy around the two separate concepts of cyber crime and information assurance. This entails the centralization and rationalization of the variety of risk and threat management enterprises across the UK government. Previous strategies that dealt with cyber crime and information assurance would seem to cover much of what the *Cyber Security Strategy* deals with, notwithstanding, perhaps, the attempts to integrate both the protection of IP as a security issue and the monetization of cyber security through the creation and promotion of new industries.

In this paper we analyzed the rationality that characterizes strategic thinking regarding the cyber domain in the United Kingdom. We saw that the discourse over risk and threat in the cyber domain has changed over time from information warfare to information assurance and cyber crime to today's focus on cyber security. Whereas previously strategy focused on well-bounded threats that could be rationalized through the concepts of intentions and capabilities today's security environment is characterized by risk and uncertainty. This struggle for coherence is typified by a reflexivity that finds risks arising out of an engagement with future scenarios within the context of vulnerability. This changed strategic thinking, typified by risk rationality, has lead to three key

[51] Cabinet Office, *The UK Cyber Security Strategy,* 2011, p.33

practices: (1) the management of risk; (2) engagement with the future; (3) the reflexive 'boomerang effect'. The changing rationality of strategy along with the shifting meaning of security for the state in turn creates a new institutionalization of security via new discourses, practices and organizations involved in managing risk.

Securitization theory attempts to explain how issues are brought into the security domain but tells us little about the effects of such changes. However as a sensitizing device it calls attention to changes in meaning over time. Combining this approach with insights from the strategic risk rationality allows us to examine changes in the institutionalization of security, cyber security and how "the logic of institutional fields come to be established." [52]

The implications of this are threefold. First, changes in the meaning of security for state actors and the prevalence of risk rationality in strategy sharpens the inherent tension between risk and threat, making the allocation of limited resources more difficult for the state. Secondly, the centrality of risk to strategy creates new organizations and practices to manage risk and to engage in working the future and generating new scenarios. Finally, the broadening of actors in the security field brings with it a growing impetus on the part of the state to maintain some semblance of control and coordination, leading to the creation of new organizations to coordinate action and rationalize policy and strategy. Yet as we see in this case study this much sought-after coordination is a difficult prospect indeed and it is not entirely clear if the functional logic of such coordination is necessary.

[52] John W. Mohr & Helene K. Lee, "From Affirmative Action to Outreach: Discourse Shifts at the University of California," Poetics 28, 2000, pp.47-71, p.51