This report is part of the RAND Corporation research report series. RAND reports present research findings and objective analysis that address the challenges facing the public and private sectors. All RAND reports undergo rigorous peer review to ensure high standards for research quality and objectivity.

RAND EUROPE

Cyber-security threat characterisation

A rapid comparative analysis

Neil Robinson, Luke Gribbon, Veronika Horvath, Kate Robertson

Prepared for the Center for Asymmetric Threat Studies (CATS),
Swedish National Defence College, Stockholm

The research described in this document was prepared for the Center for Asymmetric Threat Studies (CATS), Swedish National Defence College, Stockholm.

Published 2013 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
Westbrook Centre, Milton Road, Cambridge CB4 1YG, United Kingdom
RAND URL: http://www.rand.org
RAND Europe URL: http://www.rand.org/randeurope
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Executive summary

The Swedish National Defence College and its Center for Asymmetric Threat Studies (CATS) asked RAND Europe to undertake a rapid comparison of developed states' characterisation of cyber-security threats. This involved investigating three axes of analysis related to the integration of cyber-security within these states' broader national security and defence frameworks. The aim of this descriptive study was to act as an additional perspective and challenge to the activity underway to develop a cyber-security strategy in Sweden.

- **How are cyber threats prioritised and related to other national-level security issues across developed states?** For example, in the UK, cyber is one of the highest tier of threats within the Strategic Defence and Security Review 2010, with an allocated, defined cyber-security programme over four years, totalling £650m.[1]
- **What are the specific types of threat characterised within the cyber-security threat picture?** For example, the typology of threat actors; their strategic intent, motivation and tactical capabilities; how they have developed and responded to counter-measures; how states such as China and Russia frame their cyber-security and defence policies.
- **Who or what organisations have the policy lead in terms of roles, responsibilities and agencies' scope? What role do law enforcement agencies play, and where do they fit in this context?**

The project was limited both in size and scope and called primarily for desk research. Below, the high-level findings are summarised relating to the three questions investigated in this rapid comparative study. An overall message is that ostensible similarities in countries' cyber-security policy aims must be probed, as the research presented here suggests that they can mask differences in definitions, approaches and resultant programmes of action.

[1] UK Cabinet Office (2011).

Findings

Table E.1. Overview of the findings for the three questions

Comparator	Level of prioritisation	Characterisation of threat	Lead responding authority
Canada	One of seven highest	States (military and espionage) Cybercriminals Terrorist groups	Coordinating team within Public Safety Canada
Denmark	Highly likely	Financial damage Disruption or control of IT infrastructure and electronic warfare Espionage Cyber-relevance of terrorist threats	Sector responsibility, but leadership through the Danish Security and Intelligence Service and the National High Tech Crime Centre
Estonia	High (4 on a 5x5 matrix of impact and likelihood)	Focus on effects of threat actors	Estonian Authority for Information Systems
Finland	–	No typology available	Distributed among government departments
France	Major threat	No typology publicly used	Prime ministerial-level organisation (Agence Nationale de la Sécurité des Systems d'Information, ANSSI)
Germany	–	Terrorism, crime and war; natural hazards and technical failure or human error	Federal Ministry of the Interior and National Cyber Defence Centre (NCAZ)
The Netherlands	High priority	States Private organisations Professional criminals Terrorists Hacktivists Script kiddies Cyber-researchers Internal actors Non-actor	National Cyber Security Centre
Russian Federation	Most prominent	Internal (crime and corruption) External (state, terrorists, foreign competition)	Security Council of the Federation/Ministry of Defence National system of information protection and intelligence community
UK	Tier 1 (highest level)	Criminals Nation-states Patriotic hackers Terrorist groups Hacktivists	Cabinet Office level entity: Office for Cyber Security and Information Assurance
USA	Priority (one of four)	Criminal hackers Organised criminal groups Terrorist networks Advanced nation	Distributed across a number of organisations with inter-agency policy committee

		states	
NATO	Priority challenge (alongside four others)	None publicly available	Cyber Defence Management Board Cyber Defence Management Agency NATO's Computer Incident Response Capability
EU	–	None publicly available	Separate institutional mandates across protection of infrastructure of the EU (Computer Emergency Response Team, CERT-EU) Policy to tackle cyber-crime (DG HOME/Europol) International security and defence (European External Action Service/European Defence Agency) and business/government security (Directorate-General for Communications Networks, Content and Technology [DG CNCT]/European Network and Information Security Agency [ENISA])

Threat prioritization and relationship to other threats

For all countries examined where information was available, cyber-security threat had been prioritised highly in the top tier of security issues in national risk assessments in the last five years. However, higher prioritisation of threat has not consistently translated into greater resource allocated to the area: France, Germany, the UK and the USA have emphasised the importance of cyber-security and allocated significant cyber-specific funding streams. Others such as the Netherlands have prioritised cyber-security without making formal commitments to enhancing funding.[2] For other countries, given that cyber-security's definition in policy documents ranges from the protection of infrastructure to protection of the information society, it is highly likely that policy approaches and prioritisation will be different across states.

The findings from the case study countries provide examples of governments relating cyber threats to other areas. For example, Canada, the Netherlands and the UK have noted the migration of foreign state espionage to the cyber-environment, and are investing in responses. Moreover, in terms of impact we have identified instances where governments

[2] We were unable to obtain information for Denmark, Finland and Russia regarding spending totals, and we exclude the North Atlantic Treaty Organization (NATO) and the European Union from this part of the analysis.

are aware of the interdependencies between critical national infrastructures (eg France and the UK) and the cascade effect resulting from, for example, a cyber-attack during a natural disaster (eg Canada).

Characterisation of threat actors

With the exception of Russia, countries generally recognise a common set of threat actors, but the sophistication of the typologies of these actors vary by state. Some states such as the Netherlands have provided fuller characterisations of threat actors' motivations and targets. Additionally, countries place different emphasis on the capability and intent of these actors.

Our analysis of the development of cyber-security strategies gained from a document review suggests that cyber-security strategies are responsive to events, and hence over the last five years the emphasis has changed from a focus on transnational, terrorist threat actors to a framing of cyber-security in terms of defence and increasingly offensive capabilities against cybercriminals, state actors and their proxies. Key events which have both prompted governments to produce strategies and shaped their content include:

- the distributed denial of service (DDoS) attacks against Estonia in 2007;
- growing concern over China's digital espionage capability;
- serious and organised criminals' publicised attacks against business intellectual property;
- high-volume, low-level internet-enabled fraud; and
- the continued and intensive targeting of financial systems and governmental protectively marked information.

Governments will continue to be responsive in characterising threats; however, there is little evidence from the available literature that they have established systematic ways to forecast what future threat actors may appear on the cyber-scene.

Cyber-security leadership and the role of law enforcement authorities

Almost all of the case study countries have opted for an inter-departmental model of response to cyber-security, maintaining existing 'real world' remits in the cyberworld: for example, police managing cybercrime investigations, and security services tackling espionage. Policy leadership is commonly allocated to a coordinating body to bring together departmental responses and ensure deconfliction. In some instances these are 'new' coordinating bodies (eg Estonia and France); in others they are bolted on to existing governmental departments (UK and Canada). Overall, there is little consistency in the department assigned this role across the comparators. The body in charge of leading or coordinating policy varies from cabinet offices to interior ministries, and defence or national security directorates. There may be implications in terms of international cooperation due to this unevenness and mismatch in leadership bodies. We suggest that mapping in detail the 'hubs' of institutional cyber policy decision-making in each country would be a valuable research exercise, in order to give insight into international cooperation on cyber.

The scope of law enforcement's competences are different across states. Some have units with more developed cyber-security functions (eg France and the UK), whereas others such as Russia appear to place less emphasis on the role of mainstream policing in tackling cybercrime. Uneven consideration is given between countries to the role of computer emergency response teams (CERTs) in national response.

Going forward

The Swedish government is in the early stages of preparing to formulate its cyber-security strategy, so this report is unable to make further determinations on recommendations, other than to indicate the following:

- Use international comparisons carefully – care should be taken when leveraging practice from elsewhere, as the underlying context will be different. The Swedish government should frame how it learns from other states from the perspective of its own priorities.
- Distinguish between risk and threat – in order to properly inform responses, care needs to be taken to identify threats as threats (ie types of actor that might act strategically) and not risks (which include judgements on vulnerability and impact).
- Consider multidisciplinary approaches to threat assessment and prioritisation – an approach which uses different methods (qualitative and quantitative) could offer a more robust perspective than one that is based on single, more subjective analysis.