Minerva Center for the Rule of Law under Extreme Conditions

CYBERSECURITY PREPAREDNESS THROUGH REGULATION: A COMPARATIVE APPROACH

SUMMARY OF FIRST-STAGE RESEARCH

Researchers: Adv. Deborah Housen-Couriel, Adv. Admit Ivgi, Aurelie Amidan, Shirah Meir

Introduction

Cybersecurity preparedness is currently addressed by states and inter-governmental organizations through the application of a rapidly growing and diverse range of regulatory tools. Laws and directives continue to play a central role in this new regulatory project at the state level, yet the scope of cyber preparedness, especially for private-sector actors, also encompasses national and sectoral policy positions, standards, protocols, recommendations, best practices, fiscal tools, educational programs, trans-national enforcement mechanisms and other initiatives. The international community, as well, is moving ahead with its own transnational regulatory priorities and initiatives.

The new challenge of cybersecurity preparedness

Since the field of cybersecurity is new and poses unprecedented challenges, consensus around best practices for the prevention of cyber emergencies, their mitigation and recovery have not yet emerged in a definitive manner. Even the definition of a cyber event, or cyber emergency, is controversial in many jurisdictions. In elucidating these regulatory tools and practices, the present research, now concluding its initial stage, has identified several leading regulatory models and challenges across 14 jurisdictions, including 12 states and 2 international organizations, as follows:

- Australia
- Canada
- Estonia
- EU
- Finland
- France
- Germany
- Holland
- Israel
- Lithuania
- NATO
- Singapore
- UK
- United States

Regulatory models, competences and tools

Four regulatory models at the state level have so far emerged from the analysis, as detailed below:

(a) **broad regulation under one lead, ministerial-level agency** within a national framework supported comprehensively by both new and legacy regulators, with a relatively clear division of regulatory competences (ex. Singapore)[1];

(b) **a similar model to (a), with the lead agency sharing authority for specific cyber-related activities** with legacy regulators at the ministerial level (ex. Canada)[2];

(c) **coordination of overall regulatory policy at the ministerial level through leverage and engagement of legacy regulators** in order to meet new challenges of cybersecurity readiness (ex. Netherlands[3], Australia);

(d) **A *tabula rasa* approach** to meeting national cybersecurity challenges, with the establishment of new and distinct regulatory bodies, authorities and regulatory instruments suited to national priorities (ex. Estonia)[4].

These models are characterized by the approaches described above, with some overlap among them. Each model emphasizes a different structural approach in the state's division of labor among public institutions and private sector entities, including academia, to seven core areas of regulatory preparedness for cyber emergencies. The division of tasks manifests in terms of both the core institutions charged with preparedness, mitigation and recovery; and in terms of substantive regulatory competences and tools. In particular, the relationship among the core institutions dealing with various aspects of cybersecurity is highlighted by the graphic

[1] See, for instance, the Singapore National Cyber Security Masterplan 2018, 24 July 2013; and its National Infocomm Competency Framework (NICF), 2008 (https://www.nicf.sg/home.aspx).

[2] Canada's Public Safety ministry is the country's lead regulator for cyber preparedness, yet it shares authority for incident management, for example, with the Treasury Board; and for the government's e-services with Shared Services under the Privy Council and the Minister of Public Works and Government Services. Canada's regulatory approach also relies on an unusual degree of cooperation and information sharing between the private sector and the government, as detailed within.

[3] The Annex to the National Cyber Security Strategy 2 details these roles. The National Cyber Security Center was established in under the Ministry of Security and Justice as a governmental body providing guidance and overall coordination. See, for instance, the Singapore National Cyber Security Masterplan 2018, 24 July 2013; and its National Infocomm Competency Framework (NICF), 2008 (https://www.nicf.sg/home.aspx).

[3] Canada's Public Safety ministry is the country's lead regulator for cyber preparedness, yet it shares authority for incident management, for example, with the Treasury Board; and for the government's e-services with Shared Services under the Privy Council and the Minister of Public Works and Government Services. Canada's regulatory approach also relies on an unusual degree of cooperation and information sharing between the private sector and the government, as detailed within.

[3] The Annex to the 2013 National Cyber Security Strategy 2 details these regulatory roles. In addition, the National Cyber Security Center was established in 2011 under the Ministry of Security and Justice as a governmental body providing guidance and overall coordination, rather than regulation.

[4] The Estonian Information System Authority (RIA) was established as a subdivision of the Ministry of Economic Affairs and Communications in 2010 as the lead national agency "…for organizing protection of the state's information and communication technology … infrastructure, and exercising supervision over the security of information systems." It also regulates the protection of critical infrastructure. See Cyber Security Strategy, 2014-2017, Ministry of Economic Affairs and Communication, 2014.

representation of each jurisdiction in the interactive database that accompanies the research (see below).

Key challenges and stage two of the research project

At this point in the comparative research it is clear that, while countries have moved forward significantly over the past few years in terms of their engagement with the regulatory challenges of dealing with cyber emergencies, key challenges remain. These include:

- Effective modes of data sharing among government, commercial and international actors;
- Appropriate division of responsibility for various aspects of cyber preparedness, mitigation and recovery among governmental and private actors;
- Identification and protection of critical infrastructures, including data infrastructures;
- The "sectorization" of cyber regulation, i.e. specific arrangements for financial services and health services;
- Civil, penal and administrative responsibility for breaches of cybersecurity;
- The relationship between civilian and military cybersecurity strategies and regulation (i.e., export controls on cybersecurity equipment and services);
- Effective modes of international cooperation at both the normative and enforcement levels.

Some of these topics will be explored and analyzed in the next stage of research.

The interactive database

Finally, a unique, interactive database of regulatory institutions and tools supports the research findings discussed above (see sample below). In addition to mapping out the regulatory scheme for each of the 12 countries and 2 inter-governmental organizations studied, the database contains primary and secondary sources for each jurisdiction and for cybersecurity regulation in general. The Minerva Center is in the process of making this online tool available to researchers and practitioners.

Conclusions

While countries have moved forward significantly in terms of their engagement with the regulatory challenges of dealing with cyber emergencies, key challenges remain. Additional issues, including new modes of regulation that may be emerging to cope with new realities, and the optimal institutional structure for meeting cybersecurity challenges, have also been identified. The research identifies and analyzes these emerging trends on the basis of the comparative data studied, in addition to the four models that emerge from the comparative analysis. It is supported by an extensive database of primary and secondary sources.

***