Received: 27 February 2017 | Revised: 6 July 2017 | Accepted: 8 July 2017

DOI: 10.1111/gove.12309

ORIGINAL ARTICLE

WILEY Governance

National cyber crisis management: Different European approaches

Sergei Boeke

Universiteit Leiden Faculteit Campus Den Haag, Institute of Security and Global Affairs (ISGA)

Funding information
Municipality of The Hague; Netherlands Ministry of Defence; Ministry of Security and Justice

Cyber crises, as new forms of transboundary crises, pose serious risks to societies. This article investigates how different models of public–private partnerships shape cyber crisis management in four European countries: the Netherlands, Denmark, Estonia, and the Czech Republic. Using Provan and Kenis's modes of network governance, an initial taxonomy of cyber governance structures is provided. The Netherlands have created a participant-governed network, characterized by trust and equality. The Czech and Estonian models resemble a network administrative organization, with an enforcement role for their national cyber security centers. Denmark has adopted a lead-agency model. The article concludes that countries face two binary choices when organizing cyber defense and crisis management. First, national computer emergency response teams/computer security incident response teams can be embedded inside or outside the intelligence community. Second, cyber capacity can be centralized in one unit or spread across different sectors. These decisions fundamentally shape information-sharing arrangements and potential roles during cyber crises.

1 | INTRODUCTION

Increasing dependence on information technology and the growing interconnectedness of critical infrastructures (CIs) have led to new vulnerabilities and risks for societies. Whether instigated by malicious actors or by accident, cyber incidents have the potential to cascade and seriously disrupt the provision of essential public services. In December 2015, a Ukrainian power station was hacked and nearly a quarter of a million residents were left, albeit briefly, in the dark (Zetter, 2016). In May 2017, a ransomware attack struck more than 40 British hospitals and many other organizations across the world (Woollaston, 2017). To improve the security and resilience of their CI, states have drafted national cyber security strategies since the mid 2000s. As frameworks for setting objectives and determining how to achieve them, they have enjoyed much scholarly and policy attention (Klimburg, 2012). The institutional arrangements, however, that concern the roles and responsibilities of organizations in

cyber security and crisis management have been subject to much less academic scrutiny. This applies as much to which government organization should coordinate and implement cyber policy as it does to responsibilities in times of crises.

On a practical level, policy makers have struggled to adapt existing bureaucratic structures to information and communications technologies, with "cyber" a phenomenon that cuts across many traditional domains and competences. Invariably, in most countries a government ministry or central organization has come, by accident or design, to coordinate and/or lead national cyber security policy. This article investigates how, in four European countries—the Netherlands, Denmark, Estonia, and the Czech Republic—different government institutions have been tasked with responsibilities in cyber defense and crisis management and how they cooperate with the private sector. The cyber governance structures of these countries, except for Estonia, have enjoyed little scholarly attention, with most articles covering the Anglosphere. The countries have been selected purposefully: Each is small to medium sized and has an economy that is highly reliant on a dependable IT infrastructure. All four have an ambitious cyber policy, striving to play a leading role in their region or in the broader field of international security. Important for the comparative analysis, the political economies of these four countries do not diverge significantly, each possessing a variation of a coordinated market economy (Hall & Soskice, 2001). All four are EU and NATO members, although Denmark has an opt-out for EU Defence cooperation. As a result of global interconnectivity and the transboundary nature of cyber threats, cyber crisis management by definition includes a strong element of international cooperation.

By combining theoretical insights from the field of public administration with empirical findings on how four smaller North/Central European countries have organized cyber crisis management, this article strives to provide an initial taxonomy of governance models. The approach is incontrovertibly holistic, comprising governmental institutions, public–private partnerships, and international cooperation. There is no single blueprint for effective crisis management, but this article will offer a first conceptualization of the encountered approaches and identify some of the important institutional choices that governments face in this field.

2 | CYBER CRISIS MANAGEMENT

The field of generic crisis management encompasses the broad spectrum of prevention, mitigation and incident response, and institutional learning. While a common assumption, the further centralization of decision making is not necessarily the most effective way of addressing a crisis, with network models or decentralized authorities often more capable of judging which response would work best ('t Hart, Rosenthal, & Kouzmin, 1993). Possibilities include informal decentralization or nondecision making, and have been confirmed by much of the research since (Boin & Bynander, 2015; Boin & McConnell, 2007; Dynes & Aguirre, 2008). Crisis management is also more than just incident response, with crises increasingly regarded as processes rather than events (Pearson & Clair, 2008; Roux-Dufort, 2007). There are many different conceptual models that identify phases in the chain, with, for instance, one distinguishing five phases for effective (cyber) crisis management: prevention, preparation, containment, recovery, and learning (Kovoor-Misra & Misra, 2007).

In the four investigated countries, there is no consensus on the definition of a cyber crisis. The Netherlands, for instance, has defined an ICT crisis as a crisis that has its origin in the IT domain, that impacts on one or more CI sectors and where generic crisis management structures do not suffice (Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2012, p. 5). Building on the premise that cyber crises can also strike sectors and organizations that have not (yet) been designated national CI, this article chooses a more reductive definition, limiting the criteria of a cyber crisis to its "cyber" origin and the conviction that generic crisis management structures require adaptation to sufficiently