Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

An outlook on the institutional evolution of the European Union cyber security apparatus☆

Jukka Ruohonen*, Sami Hyrynsalmi, Ville Leppänen

Department of Information Technology, University of Turku, Turun yliopisto FI-20014, Finland

ARTICLE INFO

Article history:
Received 8 January 2016
Received in revised form 28 August 2016
Accepted 13 October 2016
Available online xxxx

Keywords:
Internet governance
Institutional change
Incident handling
CERT
CSIRT
ENISA

ABSTRACT

This paper observes the evolution of cyber security institutions recently established in the European Union. These institutions are based on older national, regional, and international Internet governance networks for voluntary transnational coordination of cyber security. The entry of the European Union in the cyber security domain caused a visible institutional change in the operational and regulatory status of the European networks, but the change was neither abrupt nor revolutionary. Rather, a new coordination hub was installed in the existing European networks, while later regulations were implemented with small incremental changes to the status of the deployed institutional hub. Building on a theoretical model of gradual institutional change from the field of political economy, the paper not only elaborates the evolution within the European Union, but also provides a political situation analysis of the contemporary technical, economic, and political challenges facing the European Union cyber security domain. Although the cyber security institution-building activities have halted or slowed down, many pressing policy issues still exist.

1. Introduction

Cyber security entered the highest level of global governance soon after the millennium. Practically all conventional global and regional forces launched different initiatives, programs, institutions, and coordination networks. In addition to individual states, this group includes the European Union (EU), the United Nations (UN), the Group of Eight and Group of Twenty, the North Atlantic Treaty Organization (NATO), and the Organisation for Economic Co-operation and Development – to point out only a few visible parties involved in the global cyber security frontier. However, in their continuing pursuit for global solutions, these traditional powers were, to a large extent, forced to coordinate their efforts with the existing technical governance institutions of the global Internet.

Coordination was also the keyword when the first cyber security institutions were introduced to the EU in the early 2000s. This paper observes the evolution of these institutions to the early 2010s. There are two goals.

The first goal is scholarly. The dual domains of cyber security and Internet governance have been both difficult to gauge via the traditional schools of thought in international relations and political science in general. Cyber security contains a bundle of theoretical and conceptual problems (Burdon, Lane, & von Nessen, 2012; Kello, 2013; von Solms & van Niekerk, 2013). For instance, the conventional theoretical means of research are difficult to apply because cyber security circumnavigates through the boundaries between public and private, military and civil, domestic and global, and, as Eriksson and Giacomello (2006) continue their listing, ultimately, between war and peace. It is arguably not even clear whether and how cyber security is different from cyber crime, cyber warfare, and related concepts. To make an explicit restriction, in this paper the focus is limited to a conventional viewpoint that is common in computer science; cyber security is taken to be about preventing or conducting technical cyber attacks that violate the confidentiality, integrity, or availability of computer systems, networks, or digital data. Crime, terrorism, privacy, intellectual property, surveillance, and related cyber-prefixed concepts are all beyond the scope of this paper.

Additional and analogous challenges have existed in the study of Internet governance. All three traditional schools in international relations (realism, idealism, and constructivism; see, e.g., Maoz, 2011) have faced theoretical challenges (Eriksson & Giacomello, 2006; Kello, 2013). The same applies to the common institutionalist approaches, which have tended to ascertain that governance occurs (only) in clearly identified institutions (van Eeten & Mueller, 2012). This paper contributes to the attempts to resolve some of these challenges with a case that is deeply rooted in the pressing security questions related to cooperative crisis management, transboundary

☆ The authors gratefully acknowledge Tekes – the Finnish Funding Agency for Innovation, DIMECC Oy, and the Cyber Trust research program for their support (grant number 3772/31/2014).

* Corresponding author.
E-mail addresses: juanruo@utu.fi (J. Ruohonen), sthyry@utu.fi (S. Hyrynsalmi), ville.leppanen@utu.fi (V. Leppänen).

http://dx.doi.org/10.1016/j.giq.2016.10.003
0740-624X/© 2016 Elsevier Inc. All rights reserved.

governance networks, and the institutionalization of multilateral venues (Bremberg, 2015). The theoretical contribution builds on celebrated (van der Heijden, 2010) theoretical framework of Streeck and Thelen (2005). By implication, the paper also joins the ongoing scholarly discussion about institutional change.

The second goal is practical. European and global developments in cyber security governance have been under close watch in the computer and engineering sciences, and, in general, at the implementation level of cyber security (Clark, Stikvoort, Stofbergen, & van den Heuvel, 2014; Hearn, 2003; Ruefle et al., 2014; Settanni et al., 2016; Skopik, Settanni, & Fiedler, 2016). When the advent of the new EU cyber security institutions have continued to puzzle political and social scientists with the overall rhetorical vagueness (Boin, Rhinard, & Ekengren, 2014; Simon & de Goede, 2015; Sliwinski, 2014), it must be that a political situation analysis cannot at least be easier on the traditional engineering side of Internet governance. To this end, the paper analyzes the contemporary technical, economic, and political challenges in the EU cyber security apparatus. The relatively new EU-level incident reporting system is used to exemplify these challenges.

The cyber security apparatus in the European Union was built upon an informal but largely technical, engineering-driven governance system between various national teams responsible for network and computer security. Because the terminology is regrettably vague regarding these teams, further remarks are warranted about the concepts used. In this paper, the term Computer Emergency Response Team (CERT) is reserved for those authoritative teams with national *and* transnational public policy responsibilities. To maintain a level of terminological rigor, the sister term Computer Security Incident Response Team (CSIRT) is used to collectively refer to the authoritative CERTs *and* all remaining incident response team types, regardless of whether they are specific to organizations, firms, or products, and irrespective whether they are coordination centers, universities and research institutions, or third-party organizations to which incident handling may be outsourced (Ruefle et al., 2014). As the abbreviations CERT and CSIRT are often used interchangeably, it should be kept in mind that this terminology manipulation is specific to this paper.

These terminology ambiguities do not undermine the scholarly relevance of the coordination networks between CSIRTs and the associated institutions. Time and time again, the coordination networks between these largely apolitical actors are touted as the path to sound global, regional, and national cyber security solutions (Choucri, Madnick, & Ferwerda, 2014; Deibert, 2011; Purser, 2011; Schaake & Vermeulen, 2016; Segal, 2013; Usmani, Mohapatra, & Prakash, 2013). It was also the group of authoritative European CERTs whose historical *modus operandi* was altered or augmented by the European Commission (EC) for regulatory purposes.

2. Theory

The theoretical viewpoint is attached to the institutionalist branches of research that have been prevalent in sociology, political science, economics, and research on Internet governance. The viewpoint draws particularly from the work conducted in the field of political economy to patch the work that was started in economics. In addition to briefly motivating the theoretical background, the forthcoming discussion frames the institutional evolution model that is contested with the case of cyber security institutions in the European Union.

2.1. Path dependency

The classical 19th- and 20th-century history in economics and social sciences contained parts that were characteristically institutionalist in their perspectives for explaining the world and the human behavior within it. In economics, for instance, this tradition was replaced by the historical emergence of mathematically oriented research. A few influential contributions brought the perspective back to the forefront economics in the 1980s, social sciences in the 1990s, and mainstream research in the 2000s and 2010s. In addition to the number of Nobel prizes that were attributed to institutionalism, a few of the early contributions are particularly noteworthy because they were based on economic analysis of technology, standards, and related aspects that were also about to revolutionize the world of the 1990s.

David's (1985) seminal article is a good example of how breakthroughs can occur from asking seemingly simple questions; why do Westerners continue to type with the QWERTY keyboard layout instead of the one August Dvorak developed? While the answers given by David (1985) were challenged for the keyboard layout case (Liebowitz & Margolis, 1995), which is arguably still a historical mystery, the theorization about path dependency had a profound impact upon understanding institutional evolution. In essence, a path may be selected more or less randomly, as was the case with QWERTY and the other classical examples, such as the VHS/Betamax debacle, but once a path is selected, it is increasingly difficult to change. The path is reproduced over and over again.

For the mathematically minded, the process is best illustrated with the famous urn of Pólya. The red and black balls that are drawn randomly from the urn shed light on the contingency and uncertainty in the selection of a path. However, if a red ball is drawn, it is put back in the urn, and another red ball is added to the urn. This sampling reflects nonergodicity and inflexibility in path dependency theory (Arthur, 1989; David, 1985). The former means that the draws are not forgotten or averaged way but are fed back into the process; the small seemingly insignificant little events are, in fact, significant. The latter term is taken to mean that the farther one has walked a red path, the harder it becomes to shift the path, to draw a black ball. If one is to influence the ultimate outcome, it is thus better to pick a path and allocate resources for it early rather than late (Besen & Farrell, 1994; Pierson, 2000). In essence, a dominant path eventually emerges, and it is difficult to alter it later.

The path dependency process is applicable to many technical phenomena. Standards, industry regulations, legacy software systems, programming languages, and operating systems might be approached by portraying them against the process. However, the theory has two logical pitfalls. First, the random events that lead to the initial path imply a logical contradiction in the sense that only history matters; the theory follows deterministically from the initial selection. Given that the initial selection of a path is seen as a random process, the theory leaves too little credit for the research of history; a path selection is a historical choice with its own historical background, whether the context is the adoption of technical standards, policies, and regulations, or the construction of cyber security institutions. The second issue follows from determinism; the theory cannot explain institutional change, which does occur, although often still slowly and largely path-dependently. In other words, path dependency theory is too deterministic and too contingent (Greener, 2002; Thelen, 1999). These limitations provoked a large amount of research on theorizing and empirically understanding institutional change and evolution.

2.2. Institutional change

The contested institutional change model is summarized in Table 1. While the theoretical model can be praised for its analytical clarity in trapping a complex phenomenon, the contribution of the model comes from its ability to tackle a large amount of scholarly research particularly in the field of political economy. Streeck and Thelen's (2005) fundamental argument builds on the observations that institutional changes are often incremental rather than