National Cybersecurity Governance and Legal Framework Case Study

Andrii Paziuk

November 2021

Copyright 2021 Andrii Paziuk. All Rights Reserved.

NO WARRANTY
THIS MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. THE AUTHOR MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. THE AUTHOR DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

Internal use. Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use. This document may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the author.

National Cybersecurity Governance and Legal Framework

Background

1. *Cybersecurity governance: general context*

National cybersecurity (CS) governance could be simply defined as exercise of cyber power and authority by all national stakeholders. It usually involves number of different departments and agencies claiming responsibility for national cybersecurity in various forms: military, law enforcement (interior), intelligence, infrastructure and other governmental and non-governmental bodies.

It is mentioned by Hathaway and Klimburg (ed. Klimburg, p. 30) that a major challenge for all national CS strategies is improving the coordination between the governmental agencies to ensure the Whole of Government effort. It could be achieved by a number of methods, such as appointment of a lead agency or by improving the inter-departmental process. The three main working modes for the last one are coordination, cooperation and collaboration (ed. Klimburg, p. 101).

The coordination mode is mostly applicable to Whole of Government efforts, but always represents one of the greatest challenges for national cybersecurity system and requires a clear legal mandate to exercise control over functions situated in different parts of government, "to work within an environment defined by the increased diffusion of power" (ed. Klimburg, p. 103). Unclear hierarchies, unofficial mandates, and uncertain legal basis are mentioned among such conceptual challenges for national cybersecurity governance.

Good CS governance is a concept about application of good governance principles to cybersecurity provision, management and oversight by national government. The guiding principles include but not limited to:

- Accountability
- Transparency
- Rule of law
- Participation
- Responsiveness
- Effectiveness
- Efficiency

The national cybersecurity legal framework should be built on the above principles and ensure integrity, predictability and continuality of CS governance. The nature of applicable law depends on the types of legal system and national constitutional traditions. CyBOK provides for some observations about differing sources of legal authority and how these vary in different contexts (CyBOK, p.52-53). One of the core missions of a legal regulation is to ensure all stakeholders use the legal definitions (terminology) in the same way, especially when governmental entities are involved. The national cybersecurity system is clearly defined based on the accepted legal terminology, thereby giving it legal authority..

2. Ukraine's national cybersecurity governance

The Ukraine's national cybersecurity regulatory framework includes several laws and regulations, such as the Law on the Basic Principles of Cybersecurity of Ukraine (Cybersecurity Law, 2017); the Law on the State Service for Special Communications and Information Protection of Ukraine (2006); the Executive Order of the President "Position on the National Cybersecurity Coordination Center" (2016); and the Cabinet of Ministers' resolution "Issues of the Ministry of Digital Transformation" (2019).

Ukraine's Cybersecurity Law defines the following terms:

> **Cybersecurity** ("kiberbezpeka"). "The safety of the vital interests of individuals and citizens, the society and the state during cyberspace usage, which ensures sustainable development of the information society and digital communication environment, timely detection, prevention, and neutralization of real and potential threats to the national security of Ukraine in cyberspace" (Art. 1, para. 5).
>
> **Cyber Protection** ("kiberzakhyst"). "A set of organizational, legal, engineering and technical measures, as well as measures of cryptographic and technical information protection aimed at preventing cyber incidents, detecting and protecting against cyberattacks, eliminating their consequences, restoring integrity and reliability of communication and technological systems;" (Art. 1, para. 7).[1]
>
> **Cyber Defense** ('kiberoborona"). "A set of political, economic, social, military, scientific, and technical, information, legal, organizational, and other measures that are taken in cyberspace and aimed at ensuring the protection of sovereignty and national defense capability, preventing armed conflict and repelling armed aggression" (Art. 1, para.10).

These definitions comprehensively cover cybersecurity functions aimed to ensure confidentiality, integrity, and availability of information, systems, and networks – constituting "objects of critical information infrastructure" (Art 1, para. 19). The challenges remain in clarifying the roles (who – what organization) and responsibilities (how – in what capacities) to perform such roles and tasks at the level of Ukraine's government.

Cybersecurity Law defines the legal and organizational basis, the basic principles of interactions among cybersecurity actors, assigns roles and responsibilities to nine government entities defined in the legislation as "key subjects of the national cybersecurity system" that comprise the National Cybersecurity System of Ukraine ("Whole of Government effort"). Eight of nine such entities are national security, law enforcement, or military organizations. The one non-security cybersecurity

[1] *Cyber protection* meaning has recently been corrected and recognized as one of five cybersecurity functions (Identify, Detect, *Protect*, Response, and Recover) in the recently approved secondary legislation (bylaws). See: Methodological Recommendations for Increasing the Level of Cyber Protection of Critical Information Infrastructure. SSSCIP Administration's Order of Oct 06, 2021. No. 601.

entity among key subjects of the national cybersecurity system is the National Bank of Ukraine (Central bank), an independent cybersecurity sector regulator for banking and financial markets.

In addition to these nine entities defined under Cybersecurity Law (2017), the Ministry of Digital Transformation (MDT) has been established in 2019 to foster digital development of Ukraine, improving accessibility of electronic governance ("paperless") services by using state mobile application, etc.

The MDT has increasingly asserted itself as a cybersecurity player, in part because the Vice Prime Minister, who heads the MDT, oversees State Service for Special Communications and Information Protection (SSSCIP). SSSCIP is the key governmental cybersecurity agency (semi-military organization) which oversees the compliance with information security requirements by governmental entities, including the MDT, and hosts the National Computer Security Incident Response Team (CERT-UA) serving to all sectors of economy, national security and defense sectors as well.

3. Cyber Requirements

Consider the three selected key cybersecurity entities, description of cyber roles, and their tasks).

3.1. Cyber Requirements by SSSCIP

S1. Formulate and implement state policy regarding use of state information resources for **information protection; counteracting technical intelligence; functioning, security and development of the state system of government communications**;

S2. **Formulate and implement** state policy on **cryptographic and technical protection** of information;

S3. **Formulate and implement state policy on cyber protection of state information resources and information**; the requirement for protection of which is established by law, and critical information infrastructure, **and implementation of state control in these areas**;

S4. **Creation and development of special communications systems; provisions by telecom operators of the resources** of their network for use by the state system of governmental communications, the national system of **confidential communication**, etc.

S5. *Participate* in the formulation and implementation of state policy regarding **electronic document management, identification, using e-trust services by** setting security and information protection requirements, control over requirements compliance, **conduct scheduled and unscheduled compliance inspections** on qualified providers of **e-trust services, certification centers, central certification body**;

S6. **Receive in the prescribed manner** from public authorities, local governments, lawful military entities, and enterprises, institutions and organizations, regardless

of the form of ownership, **information, documents and materials necessary to perform assigned tasks**;

S7. **Involve** specialists of state bodies, local self-government bodies, lawful military entities, and enterprises, institutions and organizations, regardless of the form of ownership, to consider issues within the power of the SSSCIP, and to **conduct joint inspections.**

S8. **Ensure functioning of the State Center for Cyber Protection and CERT-UA;** collect and analyze data on **attempts** to commit unauthorized actions against state information resources, **inform law enforcement agencies to prevent and stop** criminal offences in this sphere; **introduction of an organizational and technical model of cyber protection, measures to prevent, detect, and respond to cyber incidents and cyber-attacks and eliminate their consequences; inform about cyber threats and appropriate methods of protection against them;**

S9. **Coordinate the activities of (governmental) cybersecurity entities in relation to cyber protection.**

S10. **Ensure implementation of the information security audit** system at critical infrastructure facilities, **establish requirements for information security auditors and their certification/recertification; coordinate, organize and conduct vulnerability audits on the protection of critical infrastructure communication and technological systems.**

3.2. Cyber Requirements by MDT

M1. **Formulate and implement** public policy in digital economy, IT industry development, development of broadband Internet and telecommunications infrastructure, e-commerce and e-business, **electronic document management and administrative services, e-trust services, electronic identification, development of national electronic information resources** and interoperability, open data, development of digital skills and digital rights.

M2. **Performs role** of central public key infrastructure certification body; manage national web-platform of administrative services; electronic exchange and interaction between public entities, public registries, integrated system of e-identification, open data.

M3. **Participate** in formulation and implementation of state policy regarding use of state information resources for **information protection; counteracting technical intelligence; functioning, security and development of the state system of government communications**; **cryptographic and technical protection** of information; **protection of state information resources and information**; the requirement for protection of which is established by law, and critical information infrastructure.

M4. **Endorse candidates** for the position of CDTOs (Chief Digital Transformation Officers) –deputy chairperson of all governmental entities.

3.3. Cyber Requirements of NSDC

The NSDC is the "National Security and Defense Council" – a collective advisory body headed by the President of Ukraine. It participates in the following:

N1. **Coordinates and controls** the activities of cybersecurity entities of the **security and defense sector**.

N2. **Maintains National Cybersecurity Coordination Center (NCCC)** – operational unit of NSDC, which:

1. **Organizes development** of **National Cybersecurity Strategy and monitors its implementation**.
2. **Operational, information and analytical support** to the NSDC on cybersecurity and critical infrastructure protection.
3. **Participation in ensuring control** over the implementation of the decisions of the NSDC on cybersecurity issues of the state, enacted by the Presidential decrees.
4. **Forecast and identify** potential and real **cybersecurity threats to a state**, participate in the development of industry **cybersecurity indicators**.
5. **Develop conceptual principles and proposals** for: increasing the effectiveness of measures to **identify and eliminate** the factors that shape potential and real **cybersecurity threats**, preparing relevant programs and plans for their prevention and neutralization; **creating and operating government agency centers** and critical infrastructure facilities in accordance with unified data processing and cybersecurity technical requirements; introduction of domestic software and firmware **to implement authorized measures for cyber intelligence, cyber defense, counter-intelligence protection of state cybersecurity, and investigation of cybercrimes**.
6. **Participate in** ensuring the development and implementation of cybersecurity entities' mechanisms for **exchanging information needed to respond to cyberattacks and cyber incidents**, elimination of their factors and negative consequences
7. **Monitoring** the state of **development and implementation of national standards and technical regulations** for the application of ICTs, harmonized with EU and NATO standards.
8. **Initiate an information security audit** of state information resources and critical infrastructure; **raise the issue of conducting inspections** of the activities of collateral cybersecurity entities, in particular telecommunications operators, to meet technical requirements for the protection of information and license conditions.
9. **Participation in the organization and conduct of interagency cyber exercises and trainings** in the field of cybersecurity, development of relevant methodological documents and recommendations.

10. **Provide advisory to NSDC** on the **prioritization of tasks** for the implementation of state policy in cybersecurity sphere, **coordination** of the **mutual deployment of cybersecurity units** of the Armed Forces of Ukraine, specialized law enforcement agencies, and bringing them in readiness for execution of tasks in a **special period, in a state of war, state of emergenc**y and during the emergence of crisis situations that threaten the national security of Ukraine.

Case Study Overview

The aim of this case study is to apply risk assessment and correction plan development in class in a small-scale development project. This project is based on a real scenario (current Ukraine's cybersecurity governance system), where national policy-makers seek to improve integrity, predictability and continuality of CS governance. The learner will:

- gain an in-depth understanding of the good cybersecurity governance principles, complexity and diffusion of national cybersecurity powers;
- conduct comparative analysis of cybersecurity roles and tasks of three key cybersecurity governmental agencies;
- conduct semantic analyses of cybersecurity terminology to identify possible weakness ('vulnerability') in legal language (low clarity, gaps, overlapping, misleading, etc.);
- conduct risk assessment and develop corrective actions with the description of the re-distributed roles and tasks;
- apply CS governance principles to a new example of your choosing.

Student Instructions

Task 1. Given the background above and the information listed above, compare terminology used by the Ukraine Government to CyBOK. Explain differences and commonalities, account for terms that either organization is not using.

Task 2. Research the reading materials and clarify what cybersecurity functions (Identify, Detect, Protect, Response, and Recover) are assigned to each selected governmental entity (SSSCIP, NSDC, and MDT). Identify what tasks of each entity correspond to particular cybersecurity function. You may use a table (matrix) to show findings (possible overlap) by grouping organization's cybersecurity functions and tasks.

Task 3. Document 'vulnerabilities' in legal terminology (low clarity, gaps, overlapping, misleading, etc.) used for the description of tasks/functions of each governmental entity. You may also use a table (matrix) to show findings.

Task 4. Using your previous findings, evaluate the potential causes and problematic consequences of a cybersecurity governance system's functional failures based on the uncertainty, possibly overlapping or missing cybersecurity tasks of these entities. Consider every task and discover as many issues as possible. Define adequate tasks to fulfill the cybersecurity governance system's goals.

Task 5. Apply the legal terms and definitions, cybersecurity governance tasks to come up with a cybersecurity regulation for a small, fictitious country. You could use the same model of the distribution of tasks between two, three or more different agencies, but ensure that regulatory, managerial and inspection roles are not owned by the same entity and some checks and balances in the cybersecurity governance system are available.

Instructor notes

This is an introductory assignment sheet to be assigned for small groups of 1-3 students for 1-3 weeks following an instructional module on cybersecurity terminology, laws, and regulations.

Example solution

The main learning outcome of this case study is knowledge discovery and application. Therefore, no example solution is applicable, as the solution is what students make of it.

References

Cybersecurity and Infrastructure Agency, National Risk Management National Critical Functions (website). Available at: https://www.cisa.gov/national-critical-functions

DCAF: "Guide to Good Governance in Cybersecurity". Geneva Centre for Security Sector Governance, 2021. Available at: https://bit.ly/3BRl2a8, accessed 7 November 2021.

ENISA: "Definition of Cybersecurity – Gaps and Overlaps in Standardisation." 2015. Available at: https://www.enisa.europa.eu/publications/definition-of-cybersecurity, accessed 7 November 2021.

National Institute of Standards and Technology, NIST Risk Management Framework Overview. Available at: https://www.nist.gov/system/files/documents/2018/03/28/vickie_nist_risk_management_framework_overview-hpc.pdf

National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (April 16, 2018). Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Klimburg, A. (ed.): "National Cyber Security Framework Manual". Tallin: NATO Cooperative Cyber Defence Centre of Excellence, 2012. Doi: 9789949921119.

Spinu, N.: "Ukraine Cybersecurity Governance Assessment". DCAF, 2020. Available at: https://bit.ly/3o2H4ln, accessed 7 November 2021.

Ukrainian Cybersecurity Legal Framework. IFES, 2019. Available at: https://bit.ly/3wmDfuS, accessed 7 November 2021.