CSS Analyses in Security Policy
No. 341, May 2024

Comparing Critical Infrastructure Policy Updates

Russian attacks on Ukrainian critical infrastructure and other crises over the last few years have led to significant critical infrastructure policy developments within the EU, NATO, and Switzerland. Recent efforts to address the challenging risk landscape emphasize resilience and cooperation to reduce the impacts of disruptive events.

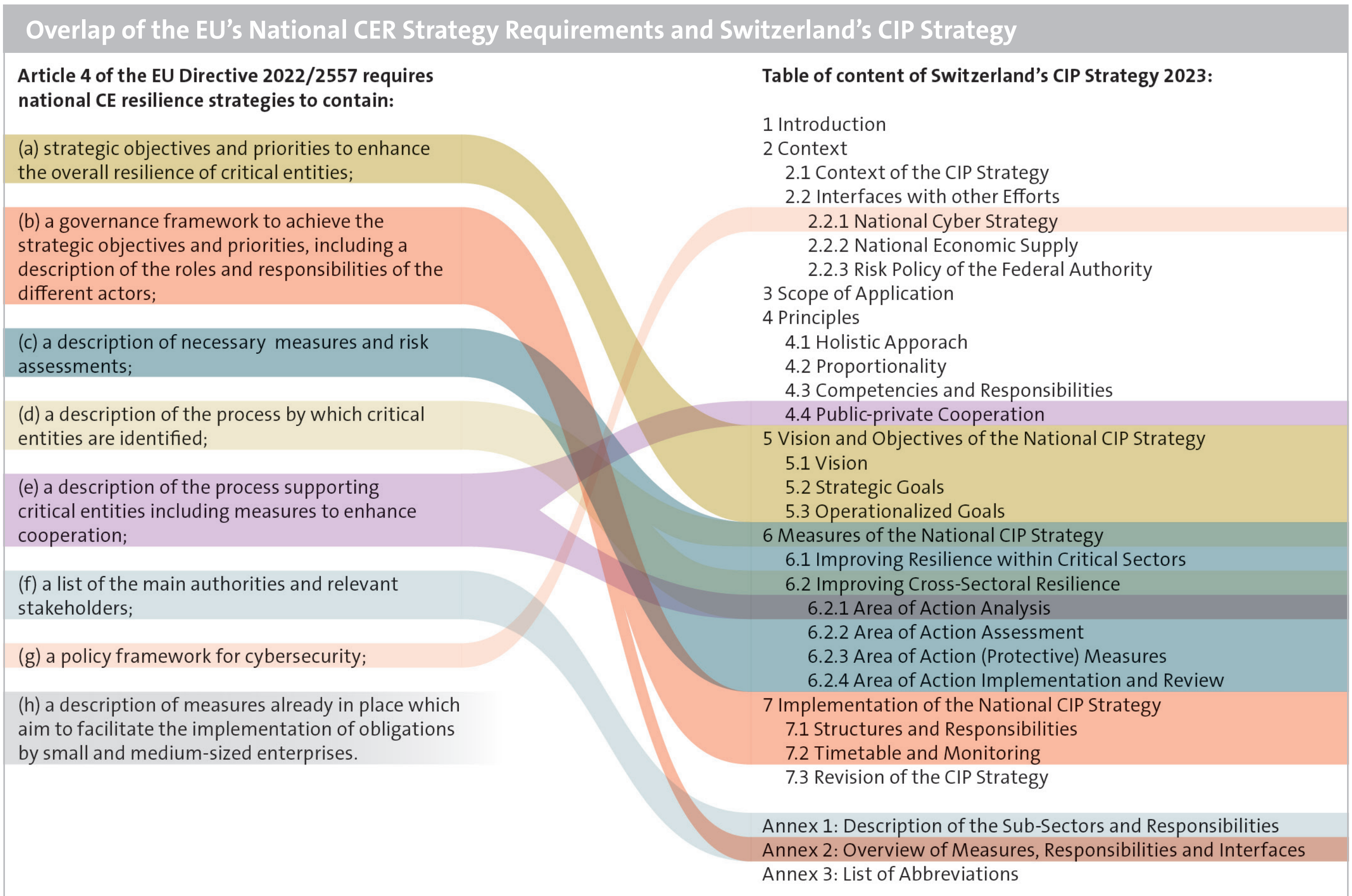
By Simon Aebi

Russia's actions in Ukraine since 2014, including their full-scale invasion in 2022, have starkly illustrated the importance of critical infrastructure (CI) and the implications of its vulnerability. For instance, Russia deliberately targeted energy and communications infrastructure to gain a military advantage by disrupting vital services to the country. However, threats to CI more often fall below the threshold of armed conflict, and are frequently labeled as "hybrid threats." These threats can arise in various forms, such as cyberattacks, espionage, disinformation, or foreign investments in infrastructure. The 2022 sabotage of the Nord Stream pipeline in the Baltic Sea has undoubtedly revealed a vulnerability in European energy infrastructure.

A presentation of, among others, the EU-NATO Task Force on Critical Infrastructure Resilience on January 11, 2023. *Johanna Geron / Reuters*

CI can be understood as the assets, systems, networks, and operators that enable and perform services necessary for the functioning of governments, economies, and societies upon which daily life depends. While different countries and organizations have slight variations in the definition and delimitation of CI, it is generally approached with a sectoral view. For example, by differentiating between energy infrastructure, communication services, or transportation networks, the sectoral view of CI offers one method to structure and organize the way CI is identified, managed, and protected. However, today's CI is characterized by strong interdependencies stemming from globalization, urbanization, digitalization, and an all-incumbent cyberspace, blurring these sectoral boundaries and making it increasingly vulnerable. For example, modern-day energy grids rely on telecommunication networks and vice versa. A disruption in energy supply could have negative implications for telecommunications. More broadly, interfering in the services provided by CI can severely affect governmental capacity, economic activities, and people's wellbeing. Potential CI disruptions stem not just from antagonistic threats but also can result from a wide range of hazards. These include natural and geophysical hazards such as floods or earthquakes and incidents caused by technical failure and human activity. For example, the train derailment involving a freight train in the Gotthard tunnel in August 2023 highlighted the impact of a disruption within the Swiss rail transportation

Overlap of the EU's National CER Strategy Requirements and Switzerland's CIP Strategy



Article 4 of the EU Directive 2022/2557 requires national CE resilience strategies to contain:

(a) strategic objectives and priorities to enhance the overall resilience of critical entities;

(b) a governance framework to achieve the strategic objectives and priorities, including a description of the roles and responsibilities of the different actors;

(c) a description of necessary measures and risk assessments;

(d) a description of the process by which critical entities are identified;

(e) a description of the process supporting critical entities including measures to enhance cooperation;

(f) a list of the main authorities and relevant stakeholders;

(g) a policy framework for cybersecurity;

(h) a description of measures already in place which aim to facilitate the implementation of obligations by small and medium-sized enterprises.

Table of content of Switzerland's CIP Strategy 2023:

1 Introduction
2 Context
2.1 Context of the CIP Strategy
2.2 Interfaces with other Efforts
2.2.1 National Cyber Strategy
2.2.2 National Economic Supply
2.2.3 Risk Policy of the Federal Authority
3 Scope of Application
4 Principles
4.1 Holistic Appoach
4.2 Proportionality
4.3 Competencies and Responsibilities
4.4 Public-private Cooperation
5 Vision and Objectives of the National CIP Strategy
5.1 Vision
5.2 Strategic Goals
5.3 Operationalized Goals
6 Measures of the National CIP Strategy
6.1 Improving Resilience within Critical Sectors
6.2 Improving Cross-Sectoral Resilience
6.2.1 Area of Action Analysis
6.2.2 Area of Action Assessment
6.2.3 Area of Action (Protective) Measures
6.2.4 Area of Action Implementation and Review
7 Implementation of the National CIP Strategy
7.1 Structures and Responsibilities
7.2 Timetable and Monitoring
7.3 Revision of the CIP Strategy

Annex 1: Description of the Sub-Sectors and Responsibilities
Annex 2: Overview of Measures, Responsibilities and Interfaces
Annex 3: List of Abbreviations

Source: EU Directive 2022/2557 and Switzerland's National CIP Strategy 2023 (adapted and translated by the author)

network. Furthermore, the Western liberalization of CI, predominantly in the 1990s, has led to CI often being held or operated by private actors. This can make governmental oversight, control, and the standardization of security measures difficult when facing cost-optimized business models.

The continuing deterioration of the international security situation has significantly increased the importance of CI and its protection among Western countries and institutions. Switzerland's Supplementary Report to the 2021 Security Policy Report, published in 2022, emphasized reviewing and adapting its strategies for resilience and cooperation in critical infrastructure protection (CIP) to be prepared for future challenges. Further, the report states that increased international cooperation, particularly with NATO and the EU, could create new opportunities to strengthen civil protection, which includes critical infrastructure protection and resilience. Consequently, reflecting on NATO and the EU's most recent changes and the current understanding of CI resilience offers a valuable point of reference to support possible or existing cooperation. Reviewing the updated national strategy on CIP of Switzerland provides a chance to observe overlaps and divergence in CIP and CI resilience concepts among Switzerland, the EU, and NATO.

From Protection to Resilience

CI resilience evolved from CIP concepts and represents a paradigm shift in the last couple of decades. CIP became a fundamental concept in security policy and described the adequate protection of CI from natural hazards, technological issues, man-made accidents, and deliberate attacks during the post-WWII and Cold War eras. CIP often pursued an all-hazards approach, attempting to identify all possible hazards and threats towards CI and mitigate those dangers. However, the all-hazards approach in CIP has its limitations as it is unrealistic and, in some instances, economically infeasible.

CI resilience, comparatively, has shifted the focus to identifying and reducing the vulnerabilities of CI. Accordingly, resilient CI is able to prevent, endure, and rebound swiftly from disruptions, ideally ensuring continuous service provision in the event of incidents and crises. Rather than attempting to protect against every possible threat or hazard, CI resilience acknowledges that not all sources of disruption can be known or anticipated. This is especially true when considering the level of interdependence and the cascading effects between CI, as well as the nature of threats within cyberspace. Furthermore, the move from CIP to CI resilience also shifted the focus from a predominantly physical asset-based view of CI to one that regards CI as systems and networks providing vital services. Today, Switzerland, the EU, and NATO have incorporated and strive for resilience in their stance on the safety and security of CI.

NATO

As an intergovernmental alliance set up for collective defense, NATO primarily focuses on mutual security and cooperation among its member states. NATO's longstanding objectives of deterrence and defense, crisis prevention, and cooperative security have, over time, increasingly become associated with the civil preparedness and national resilience of its member states. Notably, the 2016 Warsaw Summit saw NATO member states establish seven baseline requirements for resilience, including robust government functions, energy supplies, communication systems, and transport infrastructure.

The idea of achieving civil preparedness and national resilience that manifest itself in continuity of government, essential services to the population, and civil support to the military, is reemphasized again in NATO's 2022 strategic concept. As NATO includes 21 nations that are also part of the EU, the EU-NATO Task Force on the Resilience of Critical Infrastructure was established in January 2023 to take advantage of the strong linkages and shared priorities of the two institutions. The Task Force's focus thus far is on enhancing cross-institutional resilience in transportation, energy, digital infrastructure, and space through intensified cooperation, information sharing, and early warning systems. Their final assessment report, released in June 2023, provides 14 recommendations to help align the EU and NATO's approach to CI resilience. Recognizing the interconnected nature of CI, the recommendations include developing rapid, high-level responses to threats, conducting regular CI threat assessments, incorporating CI resilience topics into exercises, and promoting strategic engagement among allies, member states, and the private sector.

CI is characterized by strong interdependencies stemming from globalization, urbanization, digitalization, and an all-incumbent cyberspace

European Union

In December 2022, the European Commission replaced its 2008 Directive on CIP with its new "Critical Entities Resilience" Directive (CER). With CER, the noteworthy terminology of "critical entities" (CE) has replaced CI. Combined with the supplementary, non-exhaustive list of essential services published in 2023, CER focuses on CI operators (i.e., CE) and their services rather than the general CI sectors, as they are the ultimate object of concern. CER reflects the efforts of the EU to advance the resilience of CE and their services as crucial elements for security and defense, the EU's internal market, and the livelihood of EU citizens. To achieve this, a harmonization of national CE policies across sectors is needed. Therefore, the Directive imposes guidelines on its member states that eventually will lead to increased regulation for CE.

The relatively compressed timeline for EU member states to adopt and implement this directive further underscores the urgency of the matter. Against the backdrop of the perceived deterioration of the international security environment, CER also underlines the susceptibility of CE to hybrid threats. In addition, the Directive emphasizes the importance of and risks associated with digital and cyberspace, again reflecting an understanding of CI that goes beyond simple physical assets. Finally, CER prescribes measures to bolster the resilience of CE, such as the development of a national strategy, regular risk assessments, emergency planning, incident reporting, or support activities by authorities. In addition, strengthening collaboration and exchanging information among states, authorities, and entities must be coordinated, especially regarding emergency management.

Switzerland

In June 2023, the Federal Council published the third iteration of Switzerland's National Strategy for Critical Infrastructure Protection. The Strategy aims to align all the relevant stakeholders, from the federal to the cantonal levels and the private sector, by outlining overarching goals and principles to govern the Swiss approach to CI. Although the title indicates "critical infrastructure protection," the strategy, including its predecessor from 2017, follow the concept of CI resilience as evidenced by its vision statement: "Switzerland [being] resilient with regard to critical infrastructures so that large-scale and serious outages are prevented as far as possible or, in the event of an incident, the extent of damage is kept to a minimum." To achieve this aim, the strategy proposes eight measures, seven of which are cross-sectoral, to enhance resilience and promote cooperation between the different levels, sectors, and domains of stakeholders.

Differences in Mandate and Level

Comparing Switzerland's national strategy with NATO's recommendations as a multinational defense alliance and the EU's mandatory regulation for member states is certainly fraught with difficulties. However, doing so across their different levels of governance, enforcement, and mandate results in a more complete picture of each institution's positions and priorities *vis-à-vis* CI. First, the transferability of NATO's conception of resilience to Switzerland's CIP Strategy is limited as NATO's baseline requirements focus on the alliance's collective defense capabilities. Furthermore, the requirements outlined in the EU-NATO Task Force's final assessment report appear to simply reproduce the EU's CE approach but limited to the areas relevant to NATO's ambitions. Nevertheless, there are similarities; Switzerland's CIP strategy also spotlights resilient energy supply infrastructure, food and water resources, civil communications systems, and transport systems.

Second, whereas NATO understands resilient infrastructure as a factor that enables governments to act and communicate, the Swiss strategy emphasizes the role that prepared and resilient authorities can play in supporting CI operators if disruptive events occur, underlining the federal nature of Switzerland's political system. Third, while NATO and the EU prioritize collaboration across borders, Switzerland's strategy only briefly addresses the cross-border dependencies of CI and instead aims to guide and streamline CI resilience efforts within Switzerland. Moreover, NATO and the EU's rhetoric on potential vulnerabilities strongly emphasizes 'hybrid threats.' The Swiss strategy, comparatively, is still rather vague in defining the relevant threats and hazards and refers to national, sectoral, authority, and operator assessments instead.

Resilient CI is able to prevent, endure, and rebound swiftly from disruptions, ideally ensuring continuous service provision in the event of incidents and crises.

Fourth, the EU has adopted language that clearly marks a shift from protecting CI to the resilience of CE and the essential services they provide. While the Swiss strategy describes and aims for resilience, it nevertheless still uses the label of CI and CI operators, and the emphasis on the services is less dominant than in the CER. Fifth, the CER is a binding directive for member countries and has guidelines to be implemented by identified CE. In contrast, the

Swiss CIP is a national strategy. It is recommendatory, and any requirements or regulations arise from specific sectoral legislation (energy, transport, finance, etc.) for CI operators.

Shared Understanding

As described above, there are a number of differences between NATO's guidance, the EU's regulation, and Switzerland's strategy. Nevertheless, there is a shared understanding of the importance of CI and its resilience. Switzerland, for example, independently established and implemented approaches and measures to CI resilience that are aligned with those of both NATO and the EU. The congruence is even more obvious when comparing the EU's requirements for member countries and the Swiss CIP strategy. For example, Article 4 of the CER requires EU members to adopt a national strategy. Not only has Switzerland already had a strategy in place since 2012, but the elements required by the CER are also present in the Swiss strategy (see graphic). Moreover, the similarities go beyond just the fact of having a national strategy.

Cooperation between all stakeholders, especially in reference to private-public relations, is paramount.

First, the sectors identified as relevant to CE and CI, and that facilitate the definition of services deemed essential or critical, overlap heavily. Second, regular assessments and identification of CE or CI are asked for by both the CER and the Swiss CIP strategy, including maintaining an inventory thereof. Third, recurring risk assessments should focus on the potential disruption of services and the most effective resilience measures that may be implemented. Fourth, competent authorities that will be responsible for overseeing the implementation and supervision of the strategy must be identified, according to CER. Their role should also include supporting the relevant stakeholders and a single point of contact regarding cross-border CE issues is to be named. The Swiss strategy does this similarly, defining leading authorities and defines the Federal Office for Civil Protection as the coordinating hub for CI-related issues. Fifth, emphasis is put on information sharing and the notification of incidents that (could) disrupt service provision by the CE or CI operators. Cooperation between all stakeholders, especially in reference to private-public relations, is paramount, and enabling cross-sectoral platforms is seen to be critical to this goal. Lastly, the EU Directive advocates for national regulation to strengthen resilience. Here, the Swiss CIP strategy recommends the consideration of a proposal that would codify cross-sectoral resilience guidelines into law.

Outlook

Building upon a common understanding and similar priorities can serve as a starting point to simplify or enhance cooperation between Switzerland, NATO, and the EU, as emphasized in Switzerland's Supplementary Report to the 2021 Security Policy Report. This can be useful, especially when dealing with cross-border issues or tasks. Minimally, Switzerland must observe the CI-related developments within NATO and the EU as CIs are interconnected, and valuable lessons can be gleaned from the experiences of these organizations. NATO's ideas of national resilience and civil preparedness may be of particular interest. Relatedly, Switzerland may also learn from the EU's proposed council recommendation for a Critical Infrastructure Blueprint to enhance coordinated and cross-border responses in cases of significant incidents to CI, which is currently under discussion by the EU Council. The objective of this blueprint is to enhance shared situational awareness, better coordinate public communication, and provide effective responses to major incidents. It would be applicable when a disruptive event affects six or more Member States, or when policy coordination at the EU level is required due to the event's impact.

For more on perspectives on socio-technical resilience, see CSS core theme page.

Simon Aebi is a Senior Researcher in the Risk and Resilience Team at the Center for Security Studies (CSS) at ETH Zürich.

CSS Analyses in Security Policy is published by the Center for Security Studies (CSS) at ETH Zürich. The CSS is a center of competence for Swiss and international security policy. Each month, two analyses are published in German, French, and English.

Editor: Névine Schepers
Language editing: Allison Chandler
Layout and graphics: Miriam Dahinden-Ganzoni

Feedback and comments: analysen@sipo.gess.ethz.ch
More editions and online subscription: www.css.ethz.ch/cssanalyses

Most recent editions:

European Security Cooperation with the Indo-Pacific No. 340
Heightened Nuclear Risks and the Risk Reduction Agenda No. 339
Knowledge Security at Stake No. 338
Strategic De-risking Beyond Chips No. 337
Watching Armed Conflicts from Space No. 336
The Challenges of Wartime Polling in Ukraine No. 335

ISSN: 2296-0244; DOI: 10.3929/ethz-b-000670837