Community-Oriented Critical Infrastructure Protection TASK GROUP

/Draft Proposal by Dr Rafal Batkowski, CEO and owner at RBS;
EU Projects' Expert at University of Lodz, Poland/

Topic: Community-Oriented Critical Infrastructure Protection (CO-CIP)

Challenge:

The threat to critical infrastructure is serious and has been increasing in recent years, and the identified risks require improving national and European protection systems. In the current challenges related to building CI resilience and preventing and combating threats, including terrorist ones and those related to natural and technical incidents/disasters, we usually consider significant technological and protective resources combined with security procedures.

In this situation, it seems worth supplementing technological, organisational and management solutions with the topic of the local security environment, particularly in relation to building infrastructure resilience through effective activities with multi-stakeholders and each local community. In the longer term, ESG issues may also be related to the proposed area of activity in crisis management[1].

Goal:

The objectives of the work of the CO-CIP Task Group will include determining the potential of the local security environment in the context of identified risks and threats, the possibility of multistakeholder cooperation, assessing the vulnerability of the local environment to hostile actions aimed at CI, identifying opportunities for preventing threats and responding effectively to the threat, and examining good practices in the EU in this area. There will probably also be an opportunity to develop recommendations to enhance protective practices in line with the community-oriented CIP approach. An important issue in the next step will be programmatic action within the EU horizon and including this issue in strategic EU documents regarding CIP.

Outline:

Let's start with the essential definition: "Critical infrastructure is an asset or system essential for maintaining vital societal functions. The damage to a critical infrastructure, its destruction or disruption

[1] Compare: „ESG principles can and should be incorporated into crisis management planning. In doing so, companies can more readily respond to emerging concerns and do so more effectively. By garnering public trust and fostering creative problem solving, ESG principles can augment a company's performance in a crisis". Source: https://btlaw.com/insights/alerts/2023/improving-responses-to-crises-incorporating-esg-considerations-into-effective-crisis-management other: https://finance.ec.europa.eu/sustainable-finance/overview-sustainable-finance_en

by natural disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact on the security of the EU and the well-being of its citizens".[2]
Additionally, the **European Programme for Critical Infrastructure Protection**[3] indicates the key principles regarding CIP:

- Subsidiarity,
- Complementarity,
- Confidentiality,
- Stakeholder Cooperation,
- Proportionality,
- Sector-by-sector approach.

Treating the above Programme as a key document in the European dimension, **it does not seem to consider the issues of local communities and the importance of protective actions embedded in the realities of a specific local security environment.** The environment-oriented approach also applies to local LEAs, fire services and EMS. Only through the involvement of all stakeholders, we can ensure high resilience to threats and a professional response in the event of identifying a danger inside the facility and/or in the neighbourhood. Furthermore, from the practical point of view, communities and neighbourhoods are often the next levels up for resilience planning.
The CO-CIP Task Group should support the ecosystem of the European Cluster for Securing Critical Infrastructures - ECSCI in the form of permanent expert work and consulting to strengthen CI resilience, taking into account the needs, potential and possibilities of the local environmental activities, including challenges regarding the security of local communities, due to the neighbourhood of CI. The creation of the Task Group will help to define and then promote a sustainable approach, taking into account the needs and, on the other hand, the resources and opportunities to support CI protection by the local environment. **Task Group activities could include, for example:**

- Analyses and attempts to determine the potential of the local security environment in the context of identified risks and threats, including terrorist ones, taking into account drones with explosive devices or other hazardous materials; IED, VIED, IDD, CBRNE, etc.;
- Analyses concerning strengthening legal and practical multistakeholder cooperation;
- Vulnerability assessment tools (VAT) of the local environment to hostile actions aimed at CI - tools dedicated to EU Member States;
- Threat/crime prevention strategies and effective response in the event of danger identification - EU best practices - including in the aspect of identifying symptoms of criminal, terrorist threats as well as hybrid and asymmetric activities;
- Taking into account new technologies, including mass communication, UAVs, UGVs, etc. that can ensure a complete, coherent approach to the security of CI and neighbouring facilities, residents, etc.;
- Develop recommendations to enhance protective practices in line with the community-oriented CIP approach.

[2] https://home-affairs.ec.europa.eu/pages/page/critical-infrastructure_en
[3] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

Justification:

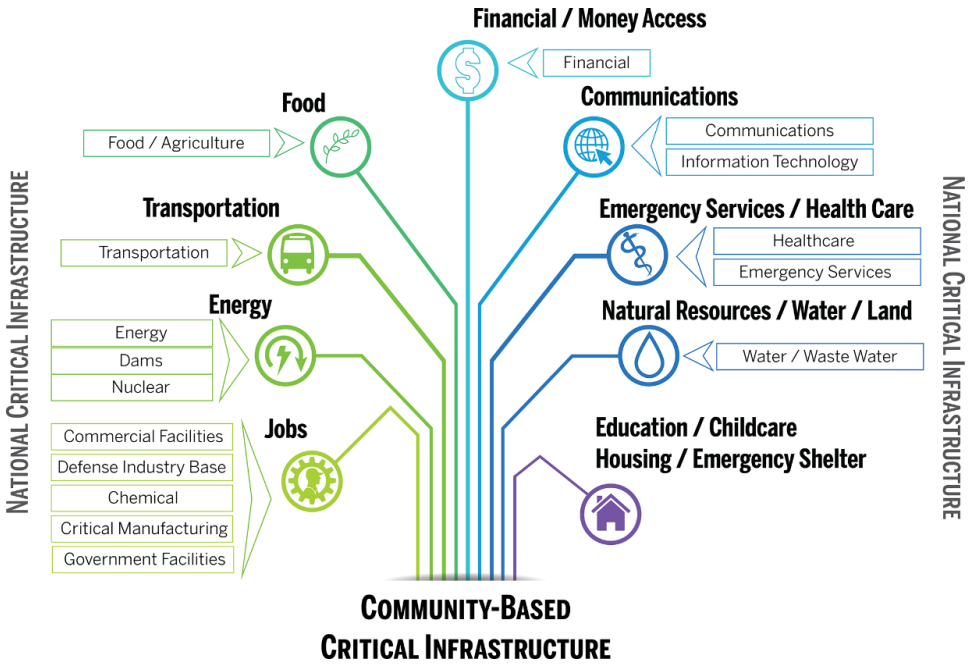
Observing the hybrid activities generated to a large extent by Russia in the areas of Ukraine, before large-scale military actions and concerning the Baltic states and Poland, their important local dimension should be emphasised. Quoting the author's work from several years ago, it should be underlined that "Experiences (...) relating to events in our region indicate that regular military operations are preceded or supplemented with sabotage (terrorist) actions in the enemy's territory intended for subordination and influencing the policy of local authorities, manipulation of social moods and behaviours of social groups and public opinion in your country, in the enemy's territory and also internationally, and, as a result, a kind of "paving the way" to take control over a territory, also using military potential. **Close observation of recent events in a neighbouring country's territory indicates the importance of the resilience of local institutions, critical infrastructure**, and services responsible for order and security to attacks, including hybrid activities that are actually characterised by terrorist tactics". It is also necessary to properly prepare local communities to deal with threat symptoms and to immediately respond to a crisis at every level of state management.

When talking about the symptoms of threats, it should be mentioned that mostly everyone is functioning in a space exposed to an attack; we should be aware of potential threats, symptoms of their occurrence, typical behaviour of perpetrators and the desired actions of each of us in the face of a threat, starting from informing the appropriate services through providing first medical aid and ending with skilful cooperation with rescuers, the Police and the Fire Services, for example when evacuating a facility, limiting access to a place or area, etc. Apart from each properly prepared person, we should remember that private/company protectors can play an important role in relation to threats and CIP. Preventive measures relevant to broadly understood crime prevention, making residents aware of how to respond to the symptoms of threats, protecting themselves against criminal activities, and strengthening the resilience of critical infrastructure should be considered vital. One of the roles of the Police defined in this way - already implemented nationwide - should be consistently strengthened.

Particularly in the context of **climate change and the digital accessibility of various services, a local community approach can be important**:[4]

[4] Compare: „From a climate emergency survival perspective, Critical Infrastructure needs to be redefined from a community-based point of view so that individual households can identify home-level Critical Infrastructure vulnerabilities and plan adaptations for increased climate emergency resilience at the household level. The sixteen 2022 Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Critical Infrastructure sectors include: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear; Transportation; and Water and Wastewater [11]. Two main factors make these federal Critical Infrastructure groupings inappropriate for community-based considerations and for use in community-based planning of adaptations for enhancing household and neighborhood level resilience.

1. The sixteen national groupings don't match community needs as perceived at the community level. For example, a home needs power. The home dweller isn't as concerned about the source of the power, the home dweller just cares that the power is being delivered to the home. From this point of view, power is a single sector. By contrast, the National Critical Infrastructure groupings have three sectors that directly generate power: Dams; Energy; and Nuclear Reactors, Materials and Waste [11].
2. The sixteen national groupings do not consider two major types of community infrastructure that are critical to communities: housing and childcare/education. Housing is an individual market that is overseen by U.S. Department of Housing and Urban Development supported variably by municipalities who provide low-



Source: https://journals.plos.org/climate/article?id=10.1371/journal.pclm.0000178

Expected Results:

- **CI managers** - more aware and ready to cooperate - taking into account the potential and opportunities, resources of local stakeholders, including each community.
- A better-prepared **local community** will be an important link in preventing threats to CI and responding to a serious attack or disaster to minimise casualties and losses. It is also important to equip members of local communities with basic knowledge and skills to identify symptoms of threats, including the activities of hostile services or criminals.
- Attention should also be paid to the need for **basic security education** of pupils and students in the above-mentioned areas and about pre-medical assistance.
- One of the important elements of **counteracting radicalisation** is social inclusion - according to the author, it is worth pointing out the postulate of ensuring organised activities aimed at the

---

income housing, homeless shelters, and community-based emergency shelters for emergencies. Education and childcare (the nurturing and preparation of our future leaders and citizenry) is primarily regulated at the state level, although Congress has passed some relevant laws influencing educational policy [12, 13]. Education and childcare, as a grouped sector, trains our future workforce, and helps instill civil, social, and ethical understanding. Education of our youth (K-12) is funded by the state but supported (through the state) by the federal government. Childcare allows parents with young children to be part of the workforce. Childcare is ultimately regulated locally and there is little to no federal or state funding to support the creation and maintenance of quality childcare beyond a childcare tax credit and funding for early childhood learning services for children in low-income families [14, 15]. Yet parents must know that their children are safe, being taken care of, fed, and educated if they are to feel free to work. Childcare and education ensure the next generation of our society will be ready to effectively enter the workforce when they reach maturity.

Society needs to reconsider the Critical Infrastructure groupings to address the perspective of communities before using Critical Infrastructure to plan adaptation strategies for climate change-induced future stressors. Using this perspective, the DHS Critical Infrastructure sectors can be grouped into super-categories, each serving specific societal and survival functions: Combined Energy sectors; Communication (combining traditional and internet); Commercial Job Sources; Financial Access; Transportation access and function; and the Military".
Source: https://journals.plos.org/climate/article?id=10.1371/journal.pclm.0000178

social inclusion of previously excluded people from the everyday, active life of local communities, potentially of interest to possible organisers of activities that threaten our community, state and all citizens. The inclusion in question is essentially intended to counteract the radicalisation of young people and ensure control over communities or individuals who may sympathise with extremist groups, ideas and activities.

Further activities:

1. Start **preparatory work for the establishment of the CO-CIP Task Group**
2. Aim to define **appropriate actions under the EPCIP** Action Plan dedicated to the issues of local environments and communities that may influence the resilience of the CIP by signalling symptoms of threats, react (e.g. inform LEAs) in the event of identifying a threat or hostile intelligence/criminal activity; limiting possible losses and victims in the event of a crisis, etc.
3. **Plan and implement a kick-off online meeting on this matter**.

In conclusion, it's to remember that the Commission has funded over 100 diverse projects under the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme (CIPS), during the 2007-2012 period. Currently, many initiatives are also being implemented to strengthen CI security. Particularly noteworthy is the **European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection - EU-CIP,** treated as an ecosystem element built as part of the European Cluster for Securing Critical Infrastructures - ECSCI.[5]

Sources (selected):

1. Jeffrey L. Ashby, Diane S. Henshel: Rethinking critical infrastructure in the United States from a community-based perspective, Published April 3, 2023. Source: https://journals.plos.org/climate/article?id=10.1371/journal.pclm.0000178
2. Lance Pierce: Civil society should be defended like other critical infrastructure; NetHope, Published August 3, 2023. Source: https://reliefweb.int/report/world/civil-society-should-be-defended-other-critical-infrastructure
3. Rafal Batkowski: Przeciwdziałanie zagrożeniom asymetrycznym i hybrydowym w perspektywie Policji [w:] Jałoszyński K., Zubrzycki W., Babiński A. (red.), Policyjne siły specjalne w Polsce, Szczytno 2015. (Counteracting asymmetric and hybrid threats from the point of view of Police).
4. Rafal Batkowski: Przeciwdziałanie terroryzmowi w lokalnym wymiarze – wybrane elementy badań własnych [w:] Wojciechowski S., Potyrała A., Bezpieczeństwo Polski. Współczesne wyzwania, Warszawa 2014. (Counteracting terrorism in the local dimension – selected elements of author's own research).
5. Rafal Batkowski: Przeciwdziałanie zagrożeniom dla Infrastruktury krytycznej [w:] Letkiewicz A. Piątek Z. (red.): Terroryzm a infrastruktura krytyczna państwa – zewnętrznego kraju Unii Europejskiej, Szczytno 2010. (Counteracting threats to critical infrastructure).
6. Chris. W. Johnson, Kevin McLean: Tools for Local Critical Infrastructure Protection: Computational Support for Identifying Safety and Security Interdependencies between Local Critical Infrastructures, Department of Computing Science, University of Glasgow, Scotland, UK, Johnson@dcs.gla.ac.uk Source: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=f658547ec2020fb489ea7734fbf078cd77e53a7d

[5] https://www.eucip.eu/