Lessons from a Didactic Table-Top Exercise During a European Training Course

Georgios THEODORIDIS
Joint Research Centre, Directorate E - Space, Security and Migration,
Unit E.02 – Technology Innovation in Security, European Commission
georgios.theodoridis@ec.europa.eu

Alexandru GEORGESCU
National Institute for Research and Development in Informatics - ICI Bucharest
alexandru.georgescu@ici.ro

Horațius-Nicolae GÂRBAN
European Security and Defence College/European External Action Service
horatius.garban@eeas.europa.eu

Abstract: This paper details the organization and conclusions of a table-top exercise which took place during a course organized under the aegis of the European Security and Defence College in February 2021. The article highlights the platform used for the exercise, the elements of the scenario and the results, stressing the importance of such exercises as a cornerstone of continuing advanced education for national and European decision makers, policy experts and specialists. Another key point is the extremely diverse group of participants, which took place, validating the idea of common training for the development of an emerging European security culture. Therefore, such training can become an added element of cooperation, especially on cyber issues, which permeated the exercise.

Keywords: Exercise, Platform, Critical infrastructure protection, Cyber, Resilience, Military mobility

INTRODUCTION

The European Security and Defence College (ESDC) of the European External Action Service, as one of its core activities, organizes European training course at different levels of seniority, technical depth and domains addressed to a diverse audience of European and national participants mainly from European and national institutions, public authorities, state but also private companies and academia. The activities are organized with the aid of various institutions and organizations in the EE which handle the development of the curriculum, the securing of speakers and many of the organizational tasks. More and more of these advanced continuing education activities for decision makers, policymakers and specialists are focusing exclusively or to a great extent on fields related to cyber, as an area of rapid change and diversification necessitating continuous educational efforts to keep up with.

In this context, on 23-25 February 2021, the European Commission's Joint Research Centre (JRC), the National Institute for Research and Development in Informatics ICI Bucharest and the Digital Security Authority of Cyprus (DSA), organized, under the aegis of the ESDC, the second module of Critical Infrastructure Protection pilot course (ESDC Activity 2020-21/255-2/1). The first module had taken place on 8-10 December 2020, titled "Emerging Technologies Transforming Critical Infrastructure Protection" (ESDC Activity 2020-21/255-1/1), and was organized by ICI Bucharest with the support of the JRC.

Due to the pandemic, the residential course format had to be abandoned and all activities took place through video teleconferencing, presenting challenges but also opportunities regarding the organization of online and offline learning, as well as the creation of added value through innovations such as additional pre-recorded lectures (given the time constraints for the course itself).

The pilot course also distinguished itself through the use of a table-top exercise not for operational or training purposes, but for didactic purposes, to reiterate and reinforce the lessons assimilated by course-goers during 2-3 days of course activities, plus the preceding days of online individual study modules and pre-recorded lectures. The scenario was programmed and run on the POSEIDON platform, a powerful tool for organizing table-top exercises in all levels of complexity, size and objectives. This paper presents the context in which the exercise took place, the tool, the scenario itself and the results and draws conclusions on the feasibility of trans-European educational programs to develop a European security culture in Critical Infrastructure Protection in general and cyber in particular.

THE COURSE CONTEXT

The second module of the course brought together 53 trainees from eleven EU Member States (Belgium, Cyprus, Czech Republic, Germany, Spain, France, Greece, Italy, Poland, Portugal and Romania) (ESDC, 2021). It took place entirely online, through WebEx videoconferencing services and also utilizing the ILIAS online education platform of the ESDC. Figure 1 is a screenshot taken during the course.

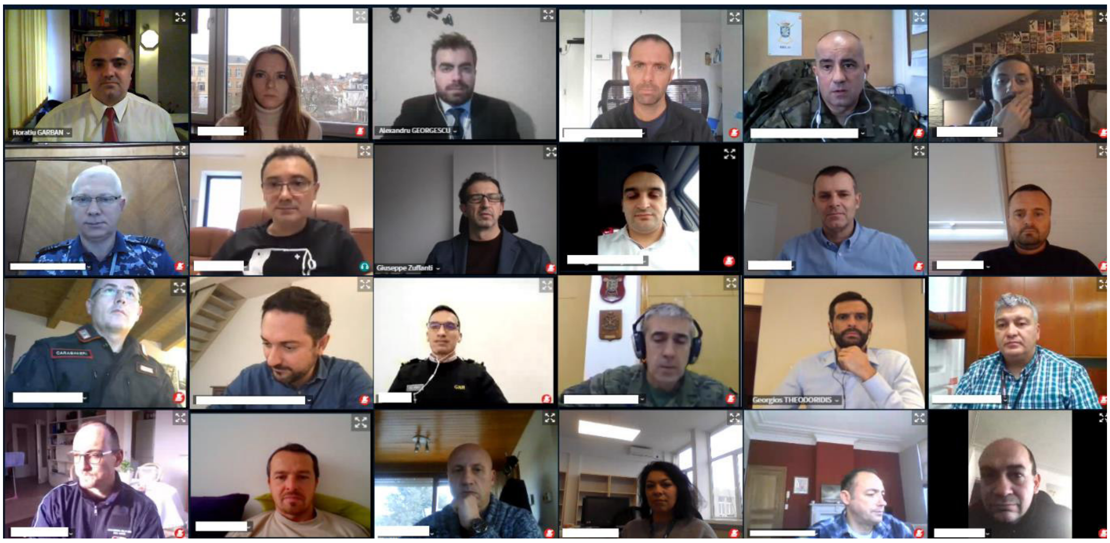


Figure 1. *Screenshot of participants during the ESDC course (source: authors)*

The overall theme of the course is Critical Infrastructure Protection and the latest developments in the area. Critical infrastructures are, according to the European Union's framework for CIP, "asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions" (European Commission, 2008). There are national critical infrastructures but also European Critical Infrastructures, whose disruption or destruction would impact two or more Member States. There are various CI taxonomies in use, but all of them contain transport, energy, food, health, finance, public administration and national defence. The European Programme for Critical Infrastructure Protection (EPCIP) has, up to this point, concerned itself with European transport and energy infrastructures, with cyber and space included through the NIS Directive and the various space programmes of the European Union. Beginning in December 2020, a new proposal is being developed for a European framework that recognizes ten areas for European Critical Infrastructures, in which "operators of essential services" and "critical entities" must be identified and actions undertaken to increase their resilience and to mitigate the risks, vulnerabilities and threats of a complex and rapidly changing security environment (European Commission, 2020).

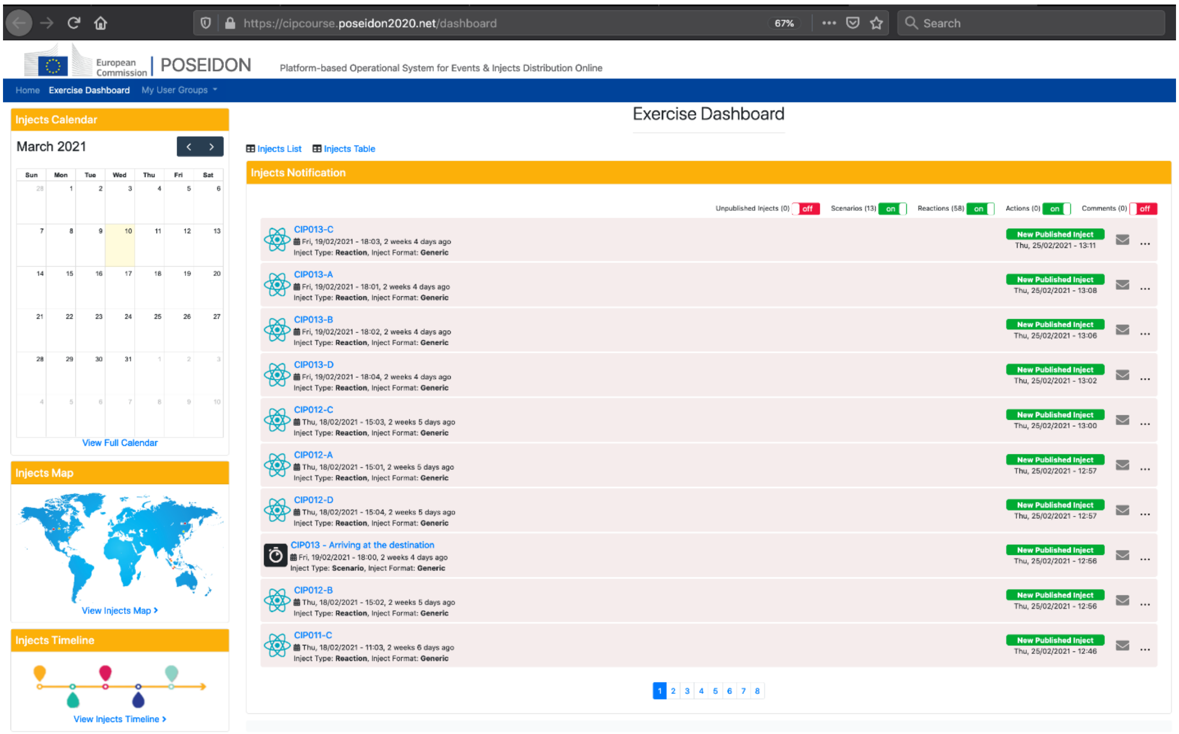
The course was addressed to "mid to high level representatives of public authorities or CI owners/operators (private and governmental) with responsibilities for the formulation and implementation of security strategies and mechanisms for Critical Infrastructure Protection" and "participants will be from the EC, from National governments of EU Member States and from state and private companies involved in CI operation" (ESDC, 2021). It provides a theoretical grounding in CIP theory, explores various subdomains of interest (such as space) which is also useful to specialists from narrow CI fields.

This particular module was dedicated to hybrid threats affecting critical cyber, energy, transport and space infrastructures and, therefore, an important emphasis was placed on exploring various hybrid aspects of the threat environment for these CI, which was also emphasized in the creation of the table-top scenario running on the Poseidon platform. Hybrid warfare, as a concept, has seen an increased attention from decision makers who are concerned with the mixing of military and non-military coercion or disruption operations, the prospects of measures "short of war", which cannot reasonably be responded to with military replies, disruptions without attribution to attackers, the ineffectiveness of deterrence and the general vulnerability of society to hybrid methods including cyber-attacks, terrorism, the dissemination of fake news and other elements. Whether it is the "unrestricted warfare" of Qiao and Yang (1999) or the "new generation warfare" (Bērziņš, 2020) developed by Russia, hybrid methods have become the preferred choice for confrontation between asymmetric adversaries for whom open battle is too expensive, risky or disruptive to countenance, or who are too interdependent to risk an open break with.

THE POSEIDON PLATFORM

The "Platform-based Operational System Events and Injects Distribution Online" (POSEIDON) was created by the Joint Research Centre of the European Commission to "support the online organization, execution, monitoring and assessment of operational exercises", including both table-top exercises and field exercises, in real time or not (JRC, 2021). It has been used in large-scale exercises, such as the Parallel and Coordinated Exercises between EU and NATO in 2018 (PACE '18). Its main advantages are the lack of specific knowledge required to work with it, rendering it very accessible to non-expert users, its customizability and capacity for enhancement with tailor-made features to accommodate exercise needs, and its low overhead, requiring only a web browser to operate (JRC, 2021). POSEIDON can be freely offered to any Member State or to any EU Institution, which can also benefit from specialty assistance from the JRC in operating or learning to operate the platform. Security is maximized through the independent running of the various exercises, and users have the option to utilize Poseidon as a service, run on the servers of the JRC, or as a product, run on their very own servers, with no information passing to the JRC. At the same time, the platform is very flexible and can accommodate numerous individuals and entities participating in exercises alone or in groups, with numerous features enabling the organization of every conceivable type of scenario.

The table-top exercise runs on the basis of programmable "injects", which may include text or multimedia content (audio/video call, background information, blog post, e-mail, episode, Facebook/Twitter post, meeting, news article, order, press release, report, TV/radio broadcast, video online, own action, website, self-discovery) and which mimic the real life process of experiencing an incident. These injects change the world state and enable individuals or groups of participants to react in a way that advances the exercise, through "reaction injects", featuring similar content, and targeted at particular individuals or groups, or through comments, leading to a dynamic scenario, advancing with the fictitious actions of participants. Figure 2 illustrates a list view of various injects and reaction injects in the Poseidon interface, taken during the exercise examined in this article.



Exercise Dashboard

Unpublished Injects (0) off   Scenarios (13) on   Reactions (58) on   Actions (0) on   Comments (0) off

CIP013-C
Fri, 19/02/2021 - 18:03, 2 weeks 4 days ago
Inject Type: **Reaction**, Inject Format: **Generic**
New Published Inject Thu, 25/02/2021 - 13:11

CIP013-A
Fri, 19/02/2021 - 18:01, 2 weeks 4 days ago
Inject Type: **Reaction**, Inject Format: **Generic**
New Published Inject Thu, 25/02/2021 - 13:08

CIP013-B
Fri, 19/02/2021 - 18:02, 2 weeks 4 days ago
Inject Type: **Reaction**, Inject Format: **Generic**
New Published Inject Thu, 25/02/2021 - 13:06

CIP013-D
Fri, 19/02/2021 - 18:04, 2 weeks 4 days ago
Inject Type: **Reaction**, Inject Format: **Generic**
New Published Inject Thu, 25/02/2021 - 13:02

CIP012-C
Thu, 18/02/2021 - 15:03, 2 weeks 5 days ago
Inject Type: **Reaction**, Inject Format: **Generic**
New Published Inject Thu, 25/02/2021 - 13:00

CIP012-A
Thu, 18/02/2021 - 15:01, 2 weeks 5 days ago
Inject Type: **Reaction**, Inject Format: **Generic**
New Published Inject Thu, 25/02/2021 - 12:57

CIP012-D
Thu, 18/02/2021 - 15:04, 2 weeks 5 days ago
Inject Type: **Reaction**, Inject Format: **Generic**
New Published Inject Thu, 25/02/2021 - 12:57

CIP013 - Arriving at the destination
Fri, 19/02/2021 - 18:00, 2 weeks 4 days ago
Inject Type: **Scenario**, Inject Format: **Generic**
New Published Inject Thu, 25/02/2021 - 12:56

CIP012-B
Thu, 18/02/2021 - 15:02, 2 weeks 5 days ago
Inject Type: **Reaction**, Inject Format: **Generic**
New Published Inject Thu, 25/02/2021 - 12:56

CIP011-C
Thu, 18/02/2021 - 11:03, 2 weeks 6 days ago
Inject Type: **Reaction**, Inject Format: **Generic**
New Published Inject Thu, 25/02/2021 - 12:46

Figure 2. *List view of various injects taken as screenshot of Poseidon platform during the exercise (source: authors)*

It is in this platform that a team composed of ICI, JRC and ESDC personnel constructed a scenario for the project participants.

THE TABLE-TOP SCENARIO

Because of logistical constraints, such as the limited time available for the course and for briefing the course participants, the decision was made to not give participants individual accounts and roles in the exercise. They were organized into four distinct groups, interacting within each other through breakout rooms, with an assigned moderator from the organizers and a JRC operator standing by to input reactions into the system.

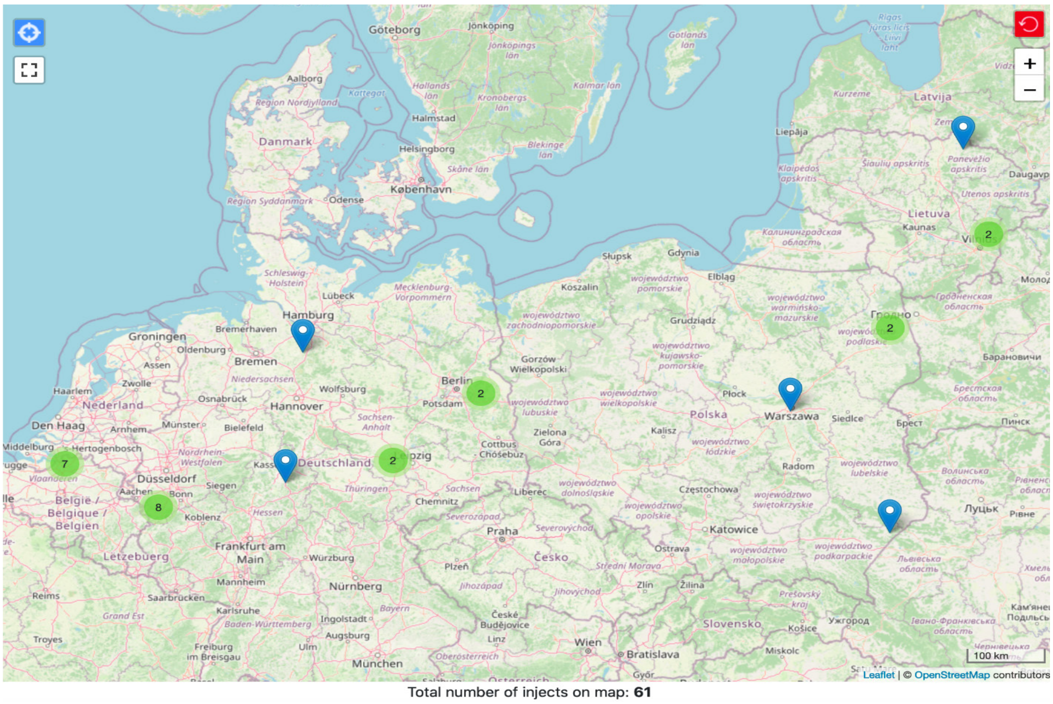
The table-top exercise was not meant to be operational, in the sense of rehearsing actionable techniques or ideas for incident management. Rather, it was didactic, providing a time-limited opportunity for participants to utilize the knowledge gained during the course in order to craft a reaction to the pre-planned injects. The exercise took, in all, over 3 hours, with another 2 hours of debrief and discussions, and was the culmination of the prior two days of theoretical lectures and small group workshops with experts in various fields related to cyber, space, energy and transportation. The scenario reflected this preoccupation on the part of the organizers of Module 2 of the Pilot Course on CIP.

The scenario runs as follows (ICI, 2021):

A military exercise with a component of military mobility is planned by the EU. Troops of EU Member States and EU allies are being moved close to the EU external borders for common exercises, in accordance with international agreements (e.g., reporting, accommodation of foreign observers etc.). Around the time of the exercise, suspicious troop movements begin to take place by EU neighbours very close to their borders with the EU. These movements, although they are presented as unannounced exercises, are actually considered to be a political statement. The EU exercise moves ahead, with troops being sent by an EU ally, Breeland, an island nation to the West of the EU. The exercise follows the military mobility portion of the exercise as it is conducted by Breeland on the territory of the EU, while heading to the military exercise sites.

As the exercise commences, a series of attempts at disruption take place as part of a hybrid campaign to challenge EU resilience and resolve. It is believed, but not proven, that the actor organizing this hybrid threat campaign (i.e., the actor behind the entities that are actually executing the individual hybrid threat attacks in various areas) is the Jamahiriya of Pasargadae, a terrorist organization looking to found a new state in the Middle East in accordance with religious tenets and to radicalize co-religionists into rejecting peaceful co-existence with people of other cultures and faiths. The terrorist organization has pre-implanted cells of operatives all over the EU, including through subsidiary organizations, sleeper groups and individuals radicalized online. The actions they plan or meant to prove the vulnerability of the EU and its allies at home, to incite fear and terror and to create political pressure against further involvement of the EU and its allies in the group's zones of interest in the Middle East. The scenario presupposes a path for the transport of troops, equipment and materiel through the Netherlands, Belgium, Germany and then Poland and the Baltics. It touches on cyber, transport, energy and space infrastructures, highlighting interdependencies and the need for national, civil-military and European coordination.

Figure 3 highlights a map view of Poseidon, with the injects that represent the dogged advance of Breeland troops and materiel across the EU, to reach the staging site for the exercise.



Total number of injects on map: **61**

Figure 3. *Map of the table-top exercise area, with scenario injects represented (Poseidon map view) (source: authors)*

Course participants were assigned to one of four categories of actors.

The four categories of actors were as follows:

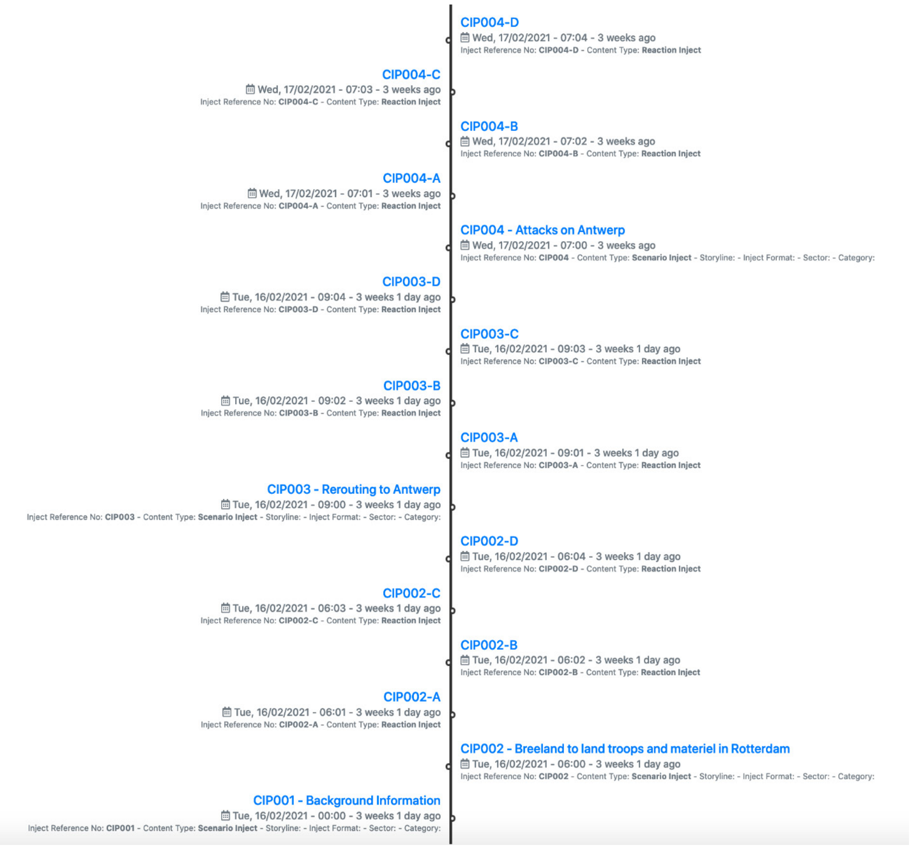
- Group A – critical infrastructure operators in all fields, private or state companies. This group had to place itself in the shoes of the CI operators, who are seeking to provide critical goods and services in a profitable manner and to maintain security of operations;
- Group B – national CIP coordinating authority – this group represented the national authorities of affected countries, either in individual sectors or in a coordinating role, such as Ministries of Interior or Ministries of Defence (given the military mobility backdrop to the exercise);
- Group C – European coordinating authority – this group represented the European authorities, either those responsible for Critical Infrastructure Protection, for crisis management, for sectoral issues like cyber-attacks and law enforcement cooperation, or for military cooperation;
- Group D – Ruthenia – this group represents an EU neighbouring country, responsible for tensions on its flank, suspicious troop movements and the fomenting of chaos in the EU neighbourhood. Ruthenia has contested the expansion of the EU in what it perceives

as its strategic near abroad and the expansion of EU security arrangements. Ruthenia is looking to amplify the chaos created by the attacks of the Jamahiriya of Pasargadae, in an opportunistic manner, also utilizing hybrid warfare elements. In this exercise, it is also one of the entities initiating suspicious troop movements and organizing unannounced exercises without Western observers. The group will list ways to aggravate the situation and prevent the stakeholders from responding in a resilient manner.

As mentioned before, it would have been too cumbersome and time consuming to manage the registration of each individual participant and the inevitable errors or logistical problems of running support activities through teleconferencing. Therefore, the participants were divided into four groups. Rather than representing individual actors (a particular institution, company, infrastructure asset operator, government), they must react to scenario injects by placing themselves in the mental modes of a particular actor type (private, national, European, opponent) and deciding their actions and postures. For example, the group representing companies owning and operating critical infrastructure will identify the infrastructure consequences of each particular inject, assume the persona of a company from that sector and geographic region, and list actions to take while inhabiting the persona of that particular actor type.

The table-top exercise:

The exercise itself consisted of 13 injects to which the four groups were supposed to react (JRC 2021). The groups had around 13 minutes to formulate a reaction to each inject, which was then logged into the system, as can be observed in figure 4.



CIP004-D
📅 Wed, 17/02/2021 - 07:04 - 3 weeks ago
Inject Reference No: **CIP004-D** - Content Type: **Reaction Inject**

CIP004-C
📅 Wed, 17/02/2021 - 07:03 - 3 weeks ago
Inject Reference No: **CIP004-C** - Content Type: **Reaction Inject**

CIP004-B
📅 Wed, 17/02/2021 - 07:02 - 3 weeks ago
Inject Reference No: **CIP004-B** - Content Type: **Reaction Inject**

CIP004-A
📅 Wed, 17/02/2021 - 07:01 - 3 weeks ago
Inject Reference No: **CIP004-A** - Content Type: **Reaction Inject**

CIP004 - Attacks on Antwerp
📅 Wed, 17/02/2021 - 07:00 - 3 weeks ago
Inject Reference No: **CIP004** - Content Type: **Scenario Inject** - Storyline: - Inject Format: - Sector: - Category:

CIP003-D
📅 Tue, 16/02/2021 - 09:04 - 3 weeks 1 day ago
Inject Reference No: **CIP003-D** - Content Type: **Reaction Inject**

CIP003-C
📅 Tue, 16/02/2021 - 09:03 - 3 weeks 1 day ago
Inject Reference No: **CIP003-C** - Content Type: **Reaction Inject**

CIP003-B
📅 Tue, 16/02/2021 - 09:02 - 3 weeks 1 day ago
Inject Reference No: **CIP003-B** - Content Type: **Reaction Inject**

CIP003-A
📅 Tue, 16/02/2021 - 09:01 - 3 weeks 1 day ago
Inject Reference No: **CIP003-A** - Content Type: **Reaction Inject**

CIP003 - Rerouting to Antwerp
📅 Tue, 16/02/2021 - 09:00 - 3 weeks 1 day ago
Inject Reference No: **CIP003** - Content Type: **Scenario Inject** - Storyline: - Inject Format: - Sector: - Category:

CIP002-D
📅 Tue, 16/02/2021 - 06:04 - 3 weeks 1 day ago
Inject Reference No: **CIP002-D** - Content Type: **Reaction Inject**

CIP002-C
📅 Tue, 16/02/2021 - 06:03 - 3 weeks 1 day ago
Inject Reference No: **CIP002-C** - Content Type: **Reaction Inject**

CIP002-B
📅 Tue, 16/02/2021 - 06:02 - 3 weeks 1 day ago
Inject Reference No: **CIP002-B** - Content Type: **Reaction Inject**

CIP002-A
📅 Tue, 16/02/2021 - 06:01 - 3 weeks 1 day ago
Inject Reference No: **CIP002-A** - Content Type: **Reaction Inject**

CIP002 - Breeland to land troops and materiel in Rotterdam
📅 Tue, 16/02/2021 - 06:00 - 3 weeks 1 day ago
Inject Reference No: **CIP002** - Content Type: **Scenario Inject** - Storyline: - Inject Format: - Sector: - Category:

CIP001 - Background Information
📅 Tue, 16/02/2021 - 00:00 - 3 weeks 1 day ago
Inject Reference No: **CIP001** - Content Type: **Scenario Inject** - Storyline: - Inject Format: - Sector: - Category:

Figure 4. *Timeline view of the exercise in Poseidon, with injects and reaction injects (source: authors)*

This section provides a summary of the data in each inject, as well as each group's reaction to that inject, which was logged into the system. The purpose of the exercise was to enable the use of accumulated knowledge and to distinguish the specific mechanisms, interests and motivations of various type of system stakeholders.

Tables 1 to 13 present the injects and the reactions of the groups, systematized to enable analysis.

Table 1. *Inject 1 of the table-top exercise on Poseidon (source: JRC)*

Identity and Time	**CIP001: [Day 1, 00:00]**
Location	European Union
Title	Background information
Description	A military exercise with a focus on military mobility is planned by the EU. Within this framework, troops of EU MS and EU allies are being moved close to the EU east external borders for common exercises, in accordance with international agreements (e.g., reporting, accommodation of foreign observers etc.). Around the time of the exercise, suspicious troop movements begin to take place by EU neighbours very close to their borders with the EU. These movements, although they are presented as unannounced exercises, are actually considered to be a political statement. The EU exercise moves ahead, with troops being sent by an EU ally, Breeland, an island nation to the West of the EU. As the exercise commences, a series of attempts at disruption take place as part of a hybrid campaign to challenge EU resilience and resolve. It is believed, but not proven, that the actor organizing this hybrid threat campaign (i.e., the actor behind the entities that are actually executing the individual hybrid threat attacks) is the Jamahiriya of Pasargadae, a terrorist organization looking to found a new state in the Middle East

Table 2. *Inject 2 of the table-top exercise on Poseidon (source: JRC)*

Identity and Time	**CIP002: [Day 1, 06:00]**
Location	Rotterdam Port
Title	Breeland to land troops and materiel in Rotterdam
Description	The exercises involve not just field operations, but also important mobility exercises to see how quickly the EU's Eastern borders may be reinforced. To that end, one of the most important components of the exercise is the transport of a consistent Breeland contingent to the live-fire exercise area utilizing dual-use infrastructure. Breeland troops, mechanized cavalry and other assets are headed to Rotterdam, where they will disembark. A few hours before disembarkation, a series of bombs go off in Rotterdam Port, affecting facilities and producing chaos. The Jamahiriya of Pasargadae claims responsibility under a religiously inspired writ to punish Europe and its allies for their involvement in the Middle East and to prove how vulnerable they are at home.

Group A reaction	Initiate pre-planned procedures for responses to bombs, fires etc, according to Operator Security Plan Contact authorities including law enforcement to secure area Assess damages and report them to the authorities to make a decision regarding the continuation of the exercise in Rotterdam. Activate emergency response teams. All operators across the EU raise the alert level given the terrorist actions Start an investigation as the operator - enemy within possibility, other forms of subversion, and to cooperate with the authorities Immediately take measures to prevent sympathetic fires and explosions, to secure dangerous substances and prevent secondary damage. Other critical infrastructure operators who are affected by the current incident must respond internally to continue or restore the provision of critical goods and services
Group B reaction	Meeting of C.I. Operators of Transport (ports, airports), Water, Energy. Request for more information. Update situational awareness. Investigate alternative solutions and ensure the safety of these alternative infrastructures. Inform the EU authorities
Group C reaction	Search for backup location, in neighbouring harbour areas and for availability next to the main port. Secretly inform all the authorities of nation to safeguard the save points, and do not give the possibility to the terrorist to know the next target of attacks. Have a few backup plans, more than 2, and send order to police department to save the areas. Discuss the possibility to use aerial vehicle to directly transfer the majority of people in order to minimize the endangering of personnel. The target is not only the harbour, but also intimidating the public. Inform the public through correct media dissemination while keeping the right balance of information to minimize adverse effects.
Group D reaction	Diplomatic response – with emphasis on the support for Ruthenia Kinetic attacks – from 2 directions Observation troops around the military movements Disinformation campaign against the Breeland exercise

Table 3. *Inject 3 of the table-top exercise on Poseidon (source: JRC)*

Identity and Time	**CIP003: [Day 1, 09:00]**
Location	Antwerp Port
Title	Rerouting to Antwerp
Description	The bomb attacks in Rotterdam Port would lead to unacceptable delays in the offloading of the Breeland troops and materiel. The attacks stiffen the resolve of the military coordinators, who decide to proceed with the exercise and to prove the resilience of the EU and its Allies, and that they will also not be intimidated by such manoeuvres. It is decided that the Breeland troops will be rerouted to Antwerp nearby, the historical rival to Rotterdam. While presenting challenges, it is believed that this will minimize delays. Antwerp Port is, however, not ready to receive them, since it did not expect such a situation.
Group A reaction	Cooperate with the Port Authority and be coordinated in a response. Perform priority assessments on existing shipping in order to see what capacity can be made available with minimal impact to current infrastructure users in order to accommodate the flow of troops and materiel Activate applicable military logistics plans from previous exercises and national or EU planning Optimize processes to accommodate all flows. Deploy teams from Rotterdam (pilots etc.), personnel to offload etc. to Antwerp to help with procedures Teams should include management and liaisons who are knowledgeable about the special cargo The Antwerp CI operator takes some precautionary risk preparedness measures for any other possible follow-up attack aiming to disrupt operations. Liaisons with the military coordinators of the exercise and liaising with the state authorities for site security
Group B reaction	Request the information from Antwerp port regarding their capacity. Coordinate with other stakeholders for enhancing the capacity of the Antwerp port. Communicate with the NL CIP authority regarding the expectations from Antwerp port. Call a meeting with all the aforementioned stakeholders. Request the plan for the further transportation of the troops out of the Antwerp port. Take the necessary actions to secure this plan (e.g., railway, roads). The time restriction (arrival of troops) should be taken into account. Use mass-media to disinform the adversary about the plan.

Group C reaction	Be in touch with the local direct cooperation for assistance. First send a group of military coordinators to check the place underwear and to prepare it for receiving us. This redirection to the second port has impact on the chain supply and touristic activity. The national trade company should organize the activities better in order to avoid civilian casualty. Separate the military activity from the civil activity. Order the Police authority to empty the roads and to minimize delays. Correctly inform the media to help citizens avoid this street.
Group D reaction	Provoke instability in the area (BE) due to ethnical issues between Provoke strikes in Antwerp port and block the physical access to the port, block some boats. Run cyber-attacks, DDoS against port, to block the functionality of the embarking and of the railway system

Table 4. *Inject 4 of the table-top exercise on Poseidon (source: JRC)*

Identity and Time	**CIP004: [Day 2, 07:00]**
Location	Antwerp Port
Title	Attacks on Antwerp
Description	The naval convoy proceeds to Antwerp. The perpetrator of the attacks, now provisionally believed to be the Jamahiriya of Pasargadae, proves its adaptability by pivoting towards disrupting the port of Antwerp. Having prioritized the European Capital for the cultivation of assets to aid in terrorist attacks, the group has significant capabilities in Belgium and knowledge of local conditions, infrastructure vulnerabilities and plans for opportunistic disruption. They mobilize a series of agents to initiate disruptive attacks. Given the timeframe and the increased alert level and scrutiny from the authorities, cyber-attacks proved to be the easiest ways to implement and attack, from a cost-benefit standpoint. Antwerp Port is affected by a series of opportunistic cyber-attacks, delaying trans-shipping efforts: • On logistics systems, making it difficult to trace containers, operate automated machinery etc.; • On electricity transmission systems, leading to brownouts in the wider Antwerp region.
Group A reaction	Notify competent authority for cyber-attacks, transport and energy. Both the port and the energy transmission company have to deal with the cyber-attack - implement procedures, activate internal cyber teams, initiate redundancies and also utilize any possible aid from the state (sectoral CERT) The port initiates countermeasures to power outage - backup generators etc.

	We need to assess the probability of collateral damage and the liabilities to the critical infrastructure operators in case of inaction Take measures to protect critical infrastructure under operation from escalating disruptions As any other energy dependent critical infrastructure operator in the Antwerp region, initiate pre-planned procedures to minimize business disruption The port and the energy company must take measures to prevent long term damage to the facility from the cyber intrusion into the industrial control systems Some facilities can be operated locally, not just centrally, but we must check to see if they have been compromised. Not all equipment is affected or is on the same level of digitalization. The same applies to the port and to energy. The incident handling teams will have been mobilized at the first sign of a cyber-attacks We must measure the attack surface and to exchange cyber threat information regarding the cyber attacks
Group B reaction	National CERT for collecting information, identifying the adequate response actions and applying these actions. Implement the national plan for communications. Ask the electricity suppliers for alternative solutions regarding alternative power provision using "manual" procedures. Alternative electricity routing. Use the military resources/infrastructure for supporting the logistics and for providing power to critical assets. Call a meeting of the Energy (electricity) operators when the power grid becomes an interconnected system of multiple operators. Call a meeting of the transport CI for the logistics part. Include also the troops' command. Inform the EU authorities. Maintain a channel of communication with the EU authorities. Communication with EU CERT.
Group C reaction	Inform the relevant authorities of EU MS about the situation. Propose MS to be ready to redirect electricity to neighbouring countries as a saver plan the save the guards. EU MS should be ready to redirect electricity to another EU MS, if needed. Get in touch with local authorities to minimize the dependency on locally automated machinery (example: call on the mobile cranes from nearby constructions). Bypass the potential effect on the local disruption caused by cyber-attacks.

	Protect the public from fake news by providing clear information about the situation from the technical side CERT and Cyber space in order to manage the situation, some IOC can prevent the attacks. Cyber-attacks – take the logistics systems of the port out of the internet, in order to enable the troop's movement on to the ships. Put the contingency plans in practice to deal with the attacks, as an effective response that will reduce the impact.
Group D reaction	Weaken the resources of the opponent. Continue the disinformation campaign – to obtain the mass movement and destroy the trust in authorities. Hack the alert channel GSM/radio and affect the alert/emergency messages. Create a political debate in disadvantage of the organization of the exercise. Diplomatic response.

Table 5. *Inject 5 of the table-top exercise on Poseidon (source: JRC)*

Identity and Time	**CIP005: [Day 2, 10:00]**
Location	Points in Germany close to the borders with Belgium
Title	Military mobility via rail
Description	Antwerp Port is part of a multimodal transport hub, with maritime, air, rail and road connections. The successful disembarkation of the maritime convoy from Breeland is followed by trans-shipment to other transport vectors. Heavy military equipment and supplies are often sent forward to the destination by rail. This is the case here as well, and several trains with tanks, other heavy equipment, and various supplies that cannot be sourced on site, are sent by rail from Antwerp in Belgium to the EU exercise staging area through Germany. Such an exercise would ordinarily involve multiple convoys making the way through the EU to the site in a coordinated fashion, but, for the purposes of this scenario, we are limiting ourselves to the Breeland contingent and the forces that join their particular convoys on their way. Germany is a "turntable" for military mobility within the EU, given its density of dual-use infrastructure built to military specifications and the numerous connections to all regions of Europe.
Group A reaction	Taking into consideration the events in Antwerp and Rotterdam, we can make some predictions regarding likelihood and type of attempted disruption of the rail transport. CI operators in general must raise the alert level to account for possible disruption of rail transport Liaise with authorities and with the internal capabilities of the rail CI operator to ensure that the rail path is clear of obstacles and damages The rail operators must coordinate and cooperate with the authorities of the host nation

	The rail operator notifies downstream critical infrastructure operators in logistics and multimodal transport to be ready for any possible disruption The military transports are prioritized not just by the host nations, but also by the companies themselves Request law enforcement and counter terror escorts from the authorities to provide security To the extent that it is possible, the CI operators must be aware of their environment and the level of security in bridges, stations etc.
Group B reaction	Enhance the communication between Belgian and German authorities by informing the German territory about the troops' movement. The Movement and Transportation Coordination Centre activated in both neighbouring countries acts according to the previously agreed procedures.
Group C reaction	Coordination among railway organizations to ensure that the electricity power will not be disturbed. The electricity needs to be supplied until the movement of the military equipment is complete (avoid power failures to the railway). Coordination should be done in advance by MS in order to redirect the electricity power from a country to another. Regroup trucks from the MS, because the next step is to lose the rails. Release counter attacks measures.
Group D reaction	Delay the rail transport. Temporary disrupt rail controls systems and power – hubs of the electrification of railway lines Temporary disconnect the control centres from the lines. Organize intelligence collection operations. Disinformation campaign used to manipulate the local political activists.

***Table 6**. Inject 6 of the table-top exercise on Poseidon (source: JRC)*

Identity and Time	CIP006: [Day 2, 11:00]
Location	Airports of Amsterdam and Brussels (origin), Vilnius and Warsaw (destination)
Title	Air transport disruption
Description	While the heavy equipment is proceeding towards the exercise areas by train, most field personnel and soldiers travel by air to reduce travel time and to get settled before the exercise. Rally points for embarkation are set in Amsterdam and Brussels, with disembarkation planned for Warsaw and Vilnius, from whence they would proceed by road to the exercise sites. As part of the concerted attempts at disruption against the military exercise of the EU and its allies, the transport by air is also targeted for disruption by the Jamahiriya of Pasargadae.

	The main vectors are through: • Cyber-attacks on radar installations in airports; • Attempted attacks on fuel depots in airports, though they are all likely to fail given the lack of preparation beforehand; • Jamming (blocking signals locally with commercially available equipment) and spoofing (faking) of GNSS signals, thereby delaying planes from taking off and from landing in safe conditions.
Group A reaction	The airport operators inform the cyber defence authorities and also deploys an incident response team The airport CI operator reroutes affected planes unable to land and delays the take off for other planes until the situation with the radar is resolved The military authorities will have to take measures to coordinate traffic by alternative means. The information of the air traffic coordination centres must be taken into account Coordination with the state authorities in transport and cyber, and also with the national and allied military coordination authorities Recall all security personnel in order to protect fuel depots and prevent more attacks. Also, request state support for this mission of protection - gendarmerie, military. Intervention teams must isolate commercial jamming and spoofing systems. Normally the effects should be eliminated based on previous provisions. There should be activated procedures related to jamming and spoofing Inform every air vehicle civilian or military around our area, about the cyber-attacks and the jamming and spoofing GNSS signals through a "clean" safe channel (maybe with the military support) in order to avoid other collateral damages Other CI operators critically dependent on air transport must initiate response procedures to minimize disruption We must handle effects on supply chains Produce cyber-attack information via internal investigation to share with the authorities and others.
Group B reaction	Increase the level of alert and implement relevant contingency plans. Ask CERTs of other EU countries (not under attack) to help resolve the situation about cyber-attacks. There are alternate GNSS and navigation services that should be activated. Call for a meeting with all the involved CI operators, including also the military, so as to make use of the military resources/infrastructure as already foreseen in the existing national contingency plan.

	Elevate the cyber incidents to the Horizontal Working Group for Cyber Incidents and ask the use of Cyber Diplomacy Toolbox to create an EU reaction.
Group C reaction	Since the GNSS is disrupted, the first measure is to land all the aircrafts of our FIR manually, by pilot's vision. Alternative sources like GLONASS or BeiDou should be used. Use local airfield with small aircrafts that fly with VFR (Visual Flight Rules) for logistic transportation. Get in touch with the national authority, EU coordinating authority for the particular approach. Alternative network for GNSS. National CERT remedies the problem promptly and Police Authority and EU authority Europol investigate it.
Group D reaction	Attack by drones in airports. Disinformation campaign and the creation of movements among airport workers – try to delay the flights. Bomb threat call in Brussels airport.

***Table** 7. Inject 7 of the table-top exercise on Poseidon (source: JRC)*

Identity and Time	**CIP007: [Day 3, 15:00]**
Location	Points in Germany
Title	Disruption of rail transport
Description	As the trains with the military equipment pass from Germany, the rail infrastructure is hit with a combination of cyber-attacks against rail management systems and physical / cyber-attacks against power stations, given the fact that the trains are electric. The purpose on the part of the attacker is to emphasize the extreme vulnerability of EU countries to disruptions of interdependent and networked critical infrastructures. The continuous harassment of the forces participating in the exercise create fears of an appearance of weakness which may encourage aggressive (and testing) behaviour on the part of systemic rivals, especially in the context of the unannounced exercises taking place simultaneously near the EU's borders and without foreign military observers.
Group A reaction	Deploy rapid reaction teams to deal with cyber-attacks (rail and energy). Share information with the authorities regarding the capabilities of the attackers. At the level which concerns the CI operators, perform foresight procedures to identify other angles of attack. The rail operator informs the authorities regarding the remediation of the problem. Other operators are on standby in case the authorities decide to change the schedule and means for mobility in order to continue the transports and demonstrate the will of the EU and its allies. Prioritize activities to conserve capacity and expedite the transportation services for the military assets.

	In the first stage of the crisis, the initial measures taken are the ones that preserve facilities, rolling stock and the lives and property of other entities. This may involve stopping the trains in the field while an investigation takes place. Adapt to the situation by switching to legacy systems such as analogue signalling and non-electric locomotives, if possible Coordinate with authorities to increase physical security by using law enforcement and other personnel in key assets Perform strategic communication with the authorities to minimize the disruption in normal operation. Affected operators need to initiate procedures to minimize disruptions from energy and transport capacity loss The affected CI operators can utilize backup and redundant capacity for energy storage or production (generators)
Group B reaction	National CERT mobilization Call a meeting of Transport and Electric Power Operators. Include also domains that are depending on the railway and which therefore suffering also from failures. Similar for the domains that are depending on the electrical power. Request Communication, collaboration, coordination at EU level in all the involved domains. Request also political reaction at EU level at different escalation degrees Consequence management.
Group C reaction	The buses remain an alternative to the train transport. When the attacks begin, activate a series of investigations among the interested MS in order to define the attributions and arrests, as recommended by EU coordination cell. This measure should be implemented simultaneously with the troops' movement for the exercise. A political statement condemning the behaviour on the part of the systemic rival in order to discourage it is also needed. The terrorist found our cyberspace vulnerability. A contingency plan with military trucks is needed to ensure the transportation of the military equipment in time for the exercise in any case. TAG has successfully intensified our vulnerabilities in cyberspace. Start taking into consideration the traditional methods. We should ensure EU's reliability which is eventually the target of the terrorists.
Group D reaction	Taking into consideration the railway disruptions, continue the Disinformation campaign – against the nations involved in the exercise. Delay/disrupt the road transport in modal points (rumours, protests). Create more chaos and discord in the society through cyber-attacks against public transport operators.

***Table 8**. Inject 8 of the table-top exercise on Poseidon (source: JRC)*

Identity and Time	**CIP008: [Day 3, 20:00]**
Location	Leipzig, Germany
Title	Road transport disruption - soft hybrid threats
Description	At the same time, light assets and more personnel move ahead by road convoy. Unlike the trains, they have to stop for the night in various locations, usually in secure military facilities of the host country, but not all the time. A hostile actor arranges for disruptive events during stops outside of secure military staging areas or close to urban areas. Protests take place along with civilian disturbances and low intensity violence. Protesters range from anti-militarists to anti-interventionists and their aggressive picketing of the encampment at a key point of vulnerability when the convoy cannot rest completely secure manages to attract global and manipulable media attention.
Group A reaction	CI operators in the nearby city, which is an agglomeration of Critical Infrastructures, should rightly fear the possibility of spillovers of riots, transformation from protests into looting and mob violence and disruption of normal operations for all CI. Operators in all possible areas, including public order and defence critical infrastructures, should take measures such as increased physical security, communication with authorities to emphasize their needs and prepare mitigation measures for the actual materialization of the threat We have to deal with a different flow of transport in the conditions in which we operate using autonomous energy sources. This affects freight flows and can create unexpected increases for passenger transport (protesters, activists, etc.). There must be coordination with the authorities. The situation may get out of hand. Depending on the level of the CI operators and their threat perception, they should initiate the application of the first stages of their contingency plans.
Group B reaction	Inform Homeland Security.
Group C reaction	The military commander of each area should cooperate with the local police commander to restrict the protesters. We should prepare the MS to receive the military convoy in order to guarantee the preparation of the next country. The EU MS will receive the convoy for this type of incidents. Keep the military convoy on major highways and secure their existence. Inform FRONTEX about any potential implication of migrants into the crisis. Propose a curfew for all the involved MSs. Release the false transport itinerary to distract the attention of the protesters.
Group D reaction	Disinformation campaign – against the leaders of the exercise (people, nations, alliances). Increase discreditation of the leaders (replace them/drop some actions). Weaken the cooperation in EU and rise the distrust in the EU authorities. Build distrust measures in EU Intelligence campaigns - increase the influence in the EU.

Table 9. Inject 9 of the table-top exercise on Poseidon (source: JRC)

Identity and Time	**CIP009: [Day 4, 10:00]**
Location	Frankfurt an der Oder, Germany
Title	Total loss of transport infrastructure
Description	As part of the campaign of the Jamahiriya of Pasargadae, a train bridge is also destroyed in order to prevent the advance of the convoy. This marks an escalation, because the bridge, as an infrastructure, is not recoverable or usable at reduced capacity.
Group A reaction	Manage the flows of rail traffic to enable the mobility of the convoy. Locate alternate routes. Coordinate with the public authorities to check for other bombs or traps. In case no accessible or advantageous routes are identified, explore the possibility of adapting to the situation by having Army Engineers set up a new bridge to pass the Oder. Cooperate with the state authorities to help in the criminal investigation of the bomb attack and to provide information required for strategic communication with the population and outside actors. Investigate the possibility of subsidiary attacks on infrastructure, aiming to cause loss of life and further permanent damage. Explore logistical options regarding the rerouting and the fragmentation of the convoy Coordination with other critical infrastructure operators must be reinforced Formulate a CI operator posture for media consumption regarding the attacks and the effects of the attack, to reinforce confidence in the infrastructure resilience Deploy security forces across the rest of the route to guard against further attacks
Group B reaction	Grave escalation. At the limits of warfare. Inform nationally for possible taking of actions at political level. Inform at EU level. Possible use of Article 42 (provision of mutual support/assistance). Ensure that the necessary safety and security measures are applied at all the CI nationally, so as to safeguard them from further attacks. Identify alternative routes for the train. Or if no such alternatives exist, other means of transportation should be identified. The alternative plan should be adequately safeguarded by the military. Include the military in all the coordination activities.
Group C reaction	Load the equipment on military trucks from Frankfurt to the next train station. Military commander cooperates with local police and helps troops disembark the train and embark on military trucks. By involving the local police, the military trucks will follow to the route without curfews and the delays will be minimized.

	EU authorities contact the national authorities. After embarking troops to the next train station, inform other MS to secure (involving local military and police forces) vulnerable spots in the next train route in order to avoid this type of incidents.
Group D reaction	Diplomatic response. Involve official media channels to announce sanctions/restrictions against EU. Influence people to aggressively pass this message to the governments, use dynamic people. Movement measures – sabotage the means of transport.

Table 10. *Inject 10 of the table-top exercise on Poseidon (source: JRC)*

Identity and Time	**CIP010: [Day 3, 09:00]**
Location	Enhancing commitments
Title	No location
Description	While the mobility portion of the exercise continues to be obstructed by the suspected coordinated campaign of the Jamahiriya of Pasargadae, tensions start running high at diplomatic level between the EU and certain of its neighbouring countries whose troop movements near EU borders seem calculated to be both suspicious and provocative. Relations deteriorate with recriminations being sent back and forth. Finally, a political decision is made in the EU and in relations with its partners to mobilize more troops for an expanded version of the exercise in the same place, planned to be sourced from various EU countries, with Breeland and other Allies currently unable to increase their contribution.
Group A reaction	The CI operators must adapt to the reality of the political decision Logistical capacity will be stressed and plans must be made in advance regarding how to handle the new influx of troops and materiel with minimum disruption to existing critical service consumers CI Operators should present authorities with an accounting of the available capacity and needs in order to cooperate to create a plan involving funding, logistical support, security for the routes The CI operators must anticipate further attempts at disruption, run in high alert level and with countermeasures and response teams in place CI operators in all sectors can anticipate the possibility of opportunistic attacks aimed at general disruption, not specific disruption of troop transports. Therefore, they will all increase their alert level The necessary measures will have to be taken in accordance with the existing logistical capacity to provide a solid response to the challenges.
Group B reaction	Increased attention should be paid by the national CIP authorities on the security of their CI, specifically for the MS at the East EU borders. EU should share info of EU countries based on possible cyber-attacks due to terrorist group cyber capacities.

	Request the assessment at EU level of the efficiency in this crisis management and the identification of possible improvements.
Group C reaction	EU ministers of Defence must have a virtual meeting to discuss the situation and to establish a common line of action. This will project the strong commitment of EU against terrorism and terrorist activities into EU territory. (and will reinforce the political decisions). HRVP should schedule meetings with the ministers of Foreign Affairs of the EU eastern counties to enhance and keep a strong connection between them. Considering the LI and the situation before this decision, the plans of these troops' movement are to be classified, by considering alternative means of transport and avenues to reach their destinations, in coordinating with other TCN. EU STRATCOM conveys the master message so that the enhancement of the exercise complies with the spirit of the EU solidarity, because EU citizen deserve protection against any internal and external threat. In addition to the previous aspects, a political decision may be taken in order to redistribute the FRONTEX forces, to assess the least dangerous areas-borders and to move the troops. The military involvement should be the last step in controlling the protests.
Group D reaction	Involve our allies to involve in diplomatic actions against EU by condemning it aggressive posture. Provoke incidents in the allied countries in order to rethink their contribution. Ask UN consultation and open debate in Security Council.

Table 11. *Inject 11 of the table-top exercise on Poseidon (source: JRC)*

Identity and Time	**CIP011: [Day 3, 11:00]**
Location	Brussels
Title	The EU calls for an emergency situation
Description	The EU declares a crisis, due to continuing border movements and political instability in border countries. Intense discussions take place in Brussels among the EU MS and the EU Institutions. This conference gives full priority to military movements and military resupplies, especially by rail. Host countries are directed to support the fast transit of the troops under safe conditions and countries must support each other if affected by attacks. The larger mobilization continues throughout the EU, now that the political decision makers have already upgraded the alert status.
Group A reaction	The CI operators must adapt to the new realities of the security environment, involving higher likelihood of attacks Implement existing security measures but also find ways to amplify them, for instance by hiring more private security, by reviewing security procedures etc.

	The CI operators must formulate a firm position to address state authorities on what level of commitment is required to prevent affecting other CI operators CI Operators must inform their downstream dependents of the possibility of interruptions or degradation of critical service provisioning Ask for clarification from state authorities regarding the prioritization of economic activity in order to reduce disruptions due to the unexpected military mobility. We must move to an operation that prioritizes the unexpected movements of resources and military personnel, but without fundamentally endangering the normal operation of the CI and its provision of services to dependents.
Group B reaction	Be informed about the outcomes of the EU-level meetings and take the necessary actions at national level based on this crisis. The actions for the MS that are not directly affected by the attacks, taking into account that EU is under attack in a general sense. The non-directly attacked MS are offering their support (expertise, resources) to further enhance the CIP of the attacked MS.
Group C reaction	Be proactive and not reactive! Cooperation is the basic element in EU. The member states of EU should find the best way to communicate each other their abilities, on the one hand, and their needs, on the other hand, in order to create a strong connection between them. Initially, the EU was born in a field of economic cooperation, but then the cooperation encompassed all the fields. Develop agility and adaptability. Start thinking the engagement of other organizations ("NATO"). Use the assets of other organizations while implementing the existing agreements. Enhance the situation awareness and overcome the confidentiality barriers both in the cyber domain and in the security and defence domain in order to enhance the effectiveness of the efforts at EU level.
Group D reaction	Diplomatic reaction – play the role of a victim, announce that we could send troops to EU border for observation and reaction to any problem. Take advantage of the financial losses due to EU Crisis. Information/disinformation campaign showing the funds that will be invested in the mobility. Launch disinformation campaigns against the army.

Table 12. *Inject 12 of the table-top exercise on Poseidon (source: JRC)*

Identity and Time	**CIP012: [Day 3, 15:00]**
Location	Points in Poland and Lithuania, close to their east borders
Title	On-site disruptions in the staging area
Description	With the steady approach of every important asset for the exercise and for deterring possible attacks on EU Member States in the current tense political situation, the Jamahiriya of Pasargadae plays one last trick up its sleeve. Its preplaced agents damage fuel depots and other supply stores that were earmarked for the exercise, looking to inflict one last debilitating blow and also affect the prestige of the EU for its handling of the crisis. This can not only attract other actors to confront the EU and gain the terrorist group some breathing room for its designs in the Middle East, but also serves as a valuable propaganda and recruitment tool.
Group A reaction	CI operators affected by this must ensure business continuity, so they must have and be ready to implement a continuity and recovery plan Increase security for facilities, especially private ones, which have not yet been affected by attacks Operators implement relevant plans and notify the authorities for support and for investigations CI operators must investigate in collaboration with the authorities if there are any insiders that are connected with the Jamahiriya of Pasargadae in order to prevent any other attacks. Coordinate with authorities to enable them to identify useful redundant or backup capacities Implement procedures to minimize facility damage and to recover as many supplies as possible From the conclusions drawn so far, additional cyber protection measures will have to be taken. The opportunistic actor is expected to take advantage of the successes of Jamahiriya Pasargadae, not only at the political level, but directly in cyberspace.
Group B reaction	Call a meeting for coordinating the use of the available resources (e.g., fuels), either with civilian or military forces. Provide information about the exact level of the impact, so that this information can be used at both national and EU level, against any disinformation/propaganda campaign that aims at falsely presenting a situation of chaos and insecurity in the EU. In general, the national CIP authorities try to trigger and contribute to the collaboration and coordination activities at EU level.
Group C reaction	EU MS should ensure the effective conduct of the exercise by suppling troops with additional fuel tanks from their reserves. The relevant EU mechanism should be activated.

	Coordination investigation EU (Europol) and national dimension (freeze all the bank accounts related to the TG in EU). Coordinate the national and EU secret service resources and proceed with preventive actions (arrests) in order to decrease the risk of further malevolent group activities.
Group D reaction	Condemn these actions and offer our support to find who stands behind these terrorist attacks. Blackmail the Jamahiriya of Pasargadae – obtain information and strengthen our position in UN, in exchange for the supplies needed to conduct their actions. Attract more people to support the actions of the JP.

Table 13. *Inject 13 of the table-top exercise on Poseidon (source: JRC)*

Identity and Time	**CIP013: [Day 4, 18:00]**
Location	Same as CIP011
Title	Arriving at the destination.
Description	The EU and its Allies have surmounted a very challenging series of attempts at disruption from the Jamahiriya of Pasargadae's assets in Europe and from opportunistic actors attracted by the possibility of inflicting additional damage with low effort and low risk of accountability. The troops, with all of their equipment, have reached the staging area, the material shortfall has been met through local and regional provisioning and the overarching crisis ends with the cessation of provocative manoeuvres on the border, as the exercise gets underway. Attacks against infrastructures end, for the moment.
Group A reaction	CI operators must lobby for an overarching EU regulation on rail safety, similar to the one for air, to provide a homogeneity for the approaches to rail. Perform immediate internal debrief, capturing ideas, impressions and data. Perform an in-depth security audit and extract lessons for security improvements to be implemented during the next Operator Security Plan review. CI operators could request from the government to create a group where every operator can share information about the situation in order to help other CI operators to prevent disruptions and to be resilient by applying new procedures and rules in their contingency plans. Solving the lingering effects on critical infrastructure to resume normal functioning CI operators should increase security capacity CI operators should support the state and European authorities in revising documents of reference like strategies to take into account the lessons learned from this crisis

Group B reaction	Maintain the level of alert, since there is a still a progressive retreat from the exercise and the attacks may continue, at general sense. Assessment, lessons-learned, suggestions for improvements. Resilience of affected infrastructures. These actions should take place at national but also at the EU-level and should include not only the technical actors, but also the political ones.
Group C reaction	Establish for the EU + MS a dedicated investigation team with members from the affected CI locations in order to gather the relevant traces and to enable a further cooperation. Besides the intention to engage within all the domains treated along the course, the potentialities expressed by the opponent groups acting along the exercises are really unrealistic.
Group D reaction	De-escalation. SWOT analysis of our actions against EU. Promote Ruthenia as peace advocate.

Following the table-top exercise, the organizers and the participant engaged in a discussion session regarding the experience of the scenario and how participants identified with their assigned stakeholder type and interacted with each other to develop actionable ideas.

As a pedagogical tool, the scenario enabled participants to consider the situations put forward using the concepts and notions imparted during the course and also to take into account the differing perspectives across the spectrum of stakeholders. At the same time, the topic of the scenario was, in itself, very current, despite the necessary liberties taken with realism for the sake of expediency. The military mobility angle was judged to be an interesting addition to the scenario and also related to specific lessons and discussions during the course. The groups were chosen in such a way as to enable inter-group homogeneity. Groups would be as diverse as possible internally, but with similarities between each other, in terms of the proportion of nationalities, civil vs military, experts vs policy implementers and so on. This was judged vital to enable rich discussions and exposure to multiple streams of opinion and thinking. Ultimately, cross-cultural and other communication issues did not come into play. The scenario was too short and the participants too flexible and results oriented to become bogged down in misunderstandings and arguments. The tables show that there were a wide variety of reactions, but they did not cover the gamut of possible answers described in the pre-drafted approaches for didactic purposes.

CONCLUSIONS

During a recent pilot course under the aegis of the ESDC on the topic of Critical Infrastructure Protection in a hybrid setting, and organized by the JRC, ICI Bucharest and the DSA of Cyprus, the course participants had the opportunity to participate collaboratively in a didactic table-top exercise. The experience was judged a success and well worth the time and effort it took to create and run the scenario, as well as the opportunity cost in terms of teaching hours for the course. Future iterations of the course will also contain such exercises, as well as the courses in other domains, since the easy handling of Poseidon and the generous terms of its use by the JRC make it an attractive option for testing knowledge even when the pandemic will have subsided and residential courses resumed.

The course fits neatly into the activities of the ESDC, to promote the development of training programmes in a European milieu, with a diverse set of organizers, participants and lecturers, thereby contributing to the emergence of a European security culture and, with it, a strategic culture as well, in time. The hybrid warfare topic is also of the utmost importance and has become a constant and constantly referenced concern for the EU, the Member States and allies and partners. Therefore, the course was a timely addition to the toolbox of the ESDC educational programmes, as well as a successfully run pilot activity in which 53 trainees from eleven EU Member States received a common high level learning experience in a complex and multidisciplinary field. Though certainly not equivalent to an actual programme or degree, a course such as this provides invaluable support for the understanding of new security concepts and realities, as well as for bridging, in the minds of participants, their areas of narrow expertise with other ones, on the basis of interdependencies, thereby making them into more effective systemic thinkers.

In the future, the EU (and its partner states), will have to significantly expand the size and scope of such programmes, especially in the cybersecurity and the critical infrastructure protection fields. The Erasmus programme for students accommodates almost one million young people each year for a learning experience in another country (EC, 2020). A similar effort must be made to give already established mid to high level decision makers and representatives the benefit of the same diverse cultural and European milieu for their efforts at continuous advanced education. This is not only necessary from the national standpoint, but also a European one, which needs to develop more than just the rudiments of a common security and strategic culture, while also preparing the human resources required to tackle a rapidly shifting security environment with novel threats and threat combinations.

REFERENCE LIST

European Commission (2020). “Erasmus Annual Report 2019”. Directorate-General for Education, Youth, Sport and Culture, Directorate R — Performance Management, Supervision and Resources;

European Commission (2008). “Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection”. 2008, 345;

European Commission (2020). “COM(2020) 829 final - Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities”. SEC(2020) 433 final - SWD(2020) 358 final - SWD(2020) 359 final, 16 December 2020;

ESDC (2021). Internal ESDC documents. European Security and Defence College;

JRC (2021). Internal JRC documents. Joint Research Centre of the EU;

ICI (2021). Internal ICI documents. National Institute for Research and Development in Informatics ICI Bucharest;

Bērziņš, J. (2020). The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria. The Journal of Slavic Military Studies, Volume 33, 2020 - Issue 3, Pages 355-380, published online on 14 Dec 2020;

Qiao, L., Wang, X. (1999). Unrestricted Warfare. PLA Literature and Arts Publishing House, February 1999.

Georgios THEODORIDIS

He received the M.Sc. and Ph.D. degrees in Electrical and Computer Engineering, with an expertise in Telecommunications, from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 2004 and 2010, respectively. Since 2013, he serves as a Scientific/Technical Project Officer at the European Commission DG Joint Research Centre, at the Directorate on Space, Security and Migration. He is involved in numerous research and development projects for policy-making support. His main research interests are in the area of Critical Infrastructure Protection (CIP), focusing on the organisation and execution of CIP exercises, review of the NIS and ECI Directives, Smart Power Grids resilience and security, EU resilience against Hybrid Threats, the cybersecurity and threat analysis and detection in the Internet Backbone, cybersecurity certification of Industrial Automation & Control Systems. In this respect, his duties also include the coordination of networks of experts in the related fields. Moreover, he is the Programme/ Project Manager for the digital transformation of important files of the EU Institutions and Member States to support policy-making and enhance the concerned regulatory and operational activities. To this end, he is responsible for the conception, design and implementation of advanced IT solutions, performing the business analysis, setting the technology strategy, and coordinating the change management and the business implementation.

Alexandru GEORGESCU

He is an Expert with the Department for Cybersecurity and Critical Infrastructure Protection of the National Institute for Research and Development in Informatics. He has an eclectic background, having studied Economics, then Geopolitics, and has obtained a PhD in Risk Engineering for Critical Infrastructure Systems. He is actively involved in advancing Critical Infrastructure Protection and Resilience issues through cooperation at international level and has worked on international projects for the European Space Agency, the Shanghai Institutes for International Studies and others. He is currently also moderating a Working Group on the Protection of Defense-related Critical Energy Infrastructures within the European Defence Agency's Consultation Forum for Sustainable Energy in the Security and Defence Sectors. He is also affiliated with the European Center for Excellence for Blockchain, with the Romanian Association for Space Technology and Industry, the EURISC Foundation and Eurodefense. Coupled with significant International exposure, he is emerging as a notable member of a new generation of Romanian security experts.

Horațius-Nicolae GÂRBAN

He is a military engineer with both Mechanical and ICT degrees, and an MSc in Cyber Security and ICT. He was seconded in 2019 as Cyber Defence Training Manager in European Security and Defence College. With more than 20 years in the cyber domain, he has the role of growing the Cyber Education, Training Exercise and Evaluation Platform and utilize its expertise in Cyber Defence and Cyber Diplomacy / External Relations in Cyber.