SecurityResearch
Community of Users

CoU Brief
Information exchange and interoperability

June 2018 / Issue 8

Summary statement

- Information exchange and interoperability is a key to empowering the operational agility of end user organisations. It is impeded by a combination of technical and transactional barriers, which range from lack of common standards to the fragmented nature of the EU security market.
- A combination of top-down and bottom-up initiatives can contribute to the realisation of 'perfect' information exchange and interoperability at the European level. Top-down initiatives present in the form of bilateral agreements, introduction of coherent standards, and strategic public procurement. Bottom-up initiatives present in the form of (among others) network and/or trust-building between organisations.
- Standards play a central role in facilitating the process of information exchange and interoperability. The key to any successful standard is the realisation of a critical mass of users. Different stakeholders can contribute, for example by enforcing standards during procurement processes (both pre-commercial and commercial), by ensuring new standards are compatible with existing technology and/or platforms, and by validating standards in real operational environment prior to their deployment. As a general rule, a good standard is easier to adhere to than it is to diverge from.
- Clear synergy exists between the various stakeholder groups' activities as they relate to interoperability. Industry, academia and research organisations can play a key role in informing standard formation and/or proposing practical implementations of interoperability solutions (sometime through research and innovation activities). These findings can (in turn) be transposed into legal frameworks and terms of reference for procurement by policymaking and practitioner circles.

Introduction

This CoU brief summarises the topic of information exchange and interoperability and relevant EU-funded projects that participated in the 11th Meeting of the Community of Users (CoU) on Secure, Safe and Resilient Societies that took place 4-7 June 2018 at the BAO convention centre in Brussels.

The Community of Users is a DG Home initiative that aims to improve information transfer of research outputs and their usability by different categories of stakeholders. During the meetings and thematic workshops, policy updates and information about H2020 projects are provided and interactive discussions are facilitated to ensure that solutions and tools resulting from research will reach users.

The thematic workshop on information exchange and interoperability, which took place on the 5th of June 2018, was a follow-up on the standardisation and common information space workshops that respectively took place during the 6th CoU Meeting in March 2017 and during the 7th CoU meeting in May 2017.

European Commission

Scope & Relevance

Information exchange and interoperability refers – in its simplest form – to different actors' ability to share information with one another and/or to coordinate their actions. At its core, 'perfect' information exchange and interoperability is desirable within the field of European security ecosystem for several reasons. First, it has the potential of increasing situational awareness. This serves not only to increase responder safety during deployments, but also to improve response rate and to optimize resource allocation. Second, in reducing the costs practitioners associate with system procurement. Third, it increases returns on investment (ROIs) on research and development (R&D) activities by reducing the chance that newly developed products will fail to generate demand. Information exchange and interoperability has been flagged as an important issue not only within the European Union and its Member States (in which, even at the national level, agencies have reported problems sharing information with their peers), but within the United States as well.

Information exchange and interoperability can present within several dimensions: transactional, technical, legal/ethical, and financial. The **transactional** dimension is comprised of organisational, political, and cultural interoperability, and concerns itself barriers to cooperation which derive from human and/or societal factors. As an example, information exchange and interoperability within the transactional domain may be impeded by one organisation's unwillingness to share data with another, or by language barriers which preclude individuals within two different organisations from effectively communicating with one-another. Information exchange and interoperability may also present at within the technical dimension. Within the **technical** dimension, interoperability concerns itself with systems' ability to share, order, and interpret information between one-another. Depending on the type of information and/or the type of system in question, barriers to technical interoperability can derive from, for example, the format in which data is saved and transmitted. Outside of factors relating to the transactional and technical dimensions of interoperability, the process may also be negatively impacted by **regulatory, legal and ethical** concerns. It is also important to note that 'perfect' interoperability is not necessarily beneficial to all actors (particularly those which deal with sensitive information and/or those which derive value from 'controlling' information), and that – as a result – the **costs** of sharing often factor into the calculus surrounding this issue.

Current debates and stakeholder perspectives

This section describes why the topic is particularly important for each stakeholder group

Practitioners

From a practitioner perspective, information exchange and interoperability – in providing organisations with information which they would otherwise not have access to – translates almost directly into an improved reaction capability at both the macro (high) and micro (low) levels and to increased operational agility. With regards to the macro level, the benefits of information interoperability present clearly in the case of the European Border and Coast Guard Agency (EBCGA), which has implemented a range of tools to mitigate challenges associated with the protection of Europe's external borders. More specifically, Frontex has addressed several issues – including the fact that many of the objects it tracks are small and the fact that many Member States lack the assets necessary to observe and/or enforce their borders – by offering standardized definitions, co-owning operational assets, and acting as a conduit through which Member State agencies can communicate operational needs (and situation pictures) with one another. This array of measures considerably enhances the collective's command & control capacity, and (in turn) has contributed significantly to reactional capacity by allowing for optimisation of the tasking & re-tasking of assets. Still, cross-border interoperability at EBCGA Coordinated Joint Operations still reveals as a major challenge and operational obstacle.

At the micro level, the benefits of interoperability present clearly in the integration of several information streams (processed social media data, drone footage, etc.) into a single operational picture which can help practitioners in navigating dangerous situations. This dynamic is clearly showcased in, for example, the Netherlands' customs office's pursuit of operational interoperability with other nations' customs offices in a bid to bolster its employees' capacity to navigate challenges such as e-commerce (which has greatly increased the volume of goods which flow through the Netherlands), the Brexit, and the current legal framework while maintaining a level playing field.

Practitioners within all categories also benefit greatly from efforts to increase information exchange and interoperability within other stakeholder groups (notably within industry and SMEs and within policymaking circles). The industry & SME and policymaker stakeholder categories respectively provide the technology which practitioners depend on (industry & SMEs) and construct the frameworks (policymakers) which defines standards that exist between countries and organisations (thus mitigating transactional barriers) and provide industry with incentives to ensure 'interoperability by design' (policymaking circles). From a practitioner perspective, the benefits associated with the aforementioned processes ranges increased ease of procurement to increased operational effectiveness and/or agility. With regards to benefits associated with ease of procurement, this has to do

with the fact that the procurement of solutions which feature 'interoperability by design' reduces the need for first responder organisations to concern themselves with technological aspects of ensuring compatibility with other systems vis-à-vis information exchange and interoperability during the procurement cycle. Increases in operational effectiveness and/or agility derive from the fact that increasing information exchange between industry & SMEs and policymakers (and, more importantly, improving the *climate* for information exchange & interoperability as a whole) has the potential of providing first responders with a wealth of data that can be integrated into operational processes.

System interoperability also reduces the costs that practitioner organisations associate with the procurement of a new system because it allows them to continue making use of existing (legacy) platforms.[1] This principle can be clearly observed within national defence procurement, where systems are designed to be compatible with existing platforms because the costs associated with replacing entire platforms would otherwise inhibit these organisations from improving their capabilities over time.

Industry & SMEs

Industry & SMEs play a central role within the field of information exchange and interoperability. This is largely because this stakeholder category can facilitate technical interoperability by proposing practical implementation of innovative systems which contemplate 'interoperability by design'. 'Interoperability by design' refers to the process of designing new systems with interoperability in mind. Depending on the product and/or system under development, this means developing it to be compatible with standards and/or existing systems with which it may need to interface during its life cycle.

While policymaking and practitioner circles can contribute to ensuring 'interoperability by design' by (among others) stipulating it as a requirement within procurement processes and by defining (and enforcing) standards (whether linguistic, cultural, legal, technical, etc.), industry actors also have a part to play. While it can be tempting to design systems which foster client dependence on the supplier (interoperability – or the domination thereof – can be a source of competition), practitioners are best served by products which a.) make use of open source (read: modular, modifiable) software, and b.) operate (where possible) within virtual environments.

Policy

Stakeholders within the policymaking category preside over several tools which can serve to alleviate challenges associated with information exchange and interoperability. First and foremost – in allocating research budgets and in defining the parameters of procurement contract – policymakers can leverage pre-commercial procurement processes (PCP) to ensure that the standards and/or technological readiness levels (TRLs) referred to within procurement notices are representative of practitioners' future needs. This achieves the twin objectives of a.) ensuring that policymakers have enough information to judge whether or not tendered proposals adhere to the principle of 'interoperability by design' (this can be achieved by allocating resources towards research into future technological requirements, currently supported standards, etc.), and b.) ensuring that bids are awarded to contractors accordingly. Second, policymakers can design (and enforce) standards (whether technological or otherwise) to – wherever possible – ensure actors have a uniform understanding of and/or behaviour towards the world. Standards – particularly when they are designed in such a way that that they are easier to adhere to than they are to diverge from – greatly increase the costs of engaging in R&D which does not pay lip service to the principle of 'interoperability by design'. This is because successful standards inevitably aggregate a critical mass of users, thus effectively rendering divergence impractical. Because European practitioner organisations continue to show hesitance when it comes to sharing sensitive information with one-another, a concrete example of necessary standardisation at the European level presents in legal frameworks that facilitate the safe exchange of such information between nations and/or agencies.

Several policy initiatives relating to improving information exchange and interoperability were discussed during the 11th CoU event on Secure, Safe and Resilient Societies that took place 4-7 June 2018 at the BAO convention centre in Brussels; namely:

- **The Union Civil Protection Mechanism.** The Union Civil Protection Mechanism (UCPM) is a framework which covers prevention, preparedness, and response that has been in place since 2001. One of the UCPM's clearest contribution to information exchange and interoperability presents in the European Response Coordination Center (ERCC), which monitors disasters around the globe and coordinates EU responses to them by connecting EU MS agencies 24/7. When a disaster occurs, the organisation can deliver assistance in the form of expertise and funding. The ERCC was mobilized a total 32 times in 2017. Expertise is provided by the EU-28 Member States, as well as Iceland, Montenegro, Norway, Serbia, the former Yugoslav Republic of Macedonia (FYROM), and Turkey, all of which committed themselves in 2015 to registering specific assets for use by the ERCC's Civil Protection Modules. Because data is often scarce when it is most valuable, the ERCC also asks Member States to share information in a relevant, reliable, timely, and simple matter. The ERCC's Analytical Sector collects data from early warning systems, ECHO field, ECHO partners, EU Del, Media, and Satellite Imagery and aggregates them to map capacity and plan to responses.

1 It should be noted that, while the pursuit of system interoperability may reduce costs in the long term, it also has the potential of increasing costs in the short term. In cases where new systems cannot be designed to integrate with legacy platforms, the adoption of a new technology and/or capability may require the adoption of a new platform. In these cases, the associated costs can be expected to be relatively high.

- **EU Interoperability framework for border management systems**. When individuals enter the EU border, several questions are of relevance. Officers need an overview of who they are, when they intend to leave, whether they have a criminal history, etc. Given the volume of individuals entering Europe today, it's almost impossible to scan these people through questionnaires. The processing of EU citizens is lubricated by EU passports, which contain information on face and fingerprints. This is not the case for extra-EU visa holders (for whom fingerprints still need to be collected, etc). This results in an overflow of biometric data which can be used to identify individuals. The framework hopes to combine the various biometric datasets in an integrated platform in order to help identify individuals which are committing identity fraud. To this end, the Commission is hoping to develop a European Search Portal which will allow the EU's various border biometric systems to aggregate data by last name. This will allow law enforcement officials to access a two-step system in which that can a.) check whether any EU system has information on a given information (returns yes/no), and b.) access all biometric information stored on an individual, should a judge grant access to actual information. The Commission has also proposed a multiple-identity detector which will register biometric data to show Green, Yellow, White, and Red individuals on the basis of whether or not they are falsifying their identity.
- **Common Information Sharing Environment (CISE).** The EU promotes information exchange between maritime surveillance systems to improved awareness as well as more efficient (and effective) operations at sea. There are more than 300 maritime authorities across member states. Under CISE, these are clustered into 7 maritime sectors (defence, safety and security, fisheries, law enforcement, customs, environmental protection, border control). CISE aims to create an **operational and technical interoperability environment** which enables **seamless and reliable information sharing** between existing and future surveillance systems. The challenge is cross-sectoral. As an example, defence data is often incompatible with data collected by fisheries. The CISE is scheduled to be fully operational by 2020, and comprises several projects (BlueMass Med, Marsuno, CoopP & Incubator, EUCISE2020). Implementation will occur on the basis of three layers of interoperability. The first is exchange between EU agencies (consolidate information reviewed from Member States). The second is the exchange between Member State and EU agencies. Finally, the third is exchange within and between Member States. Several information problems present in implementing an interoperability framework. Developing common software requires knowledge of a plethora of moving parts, including common components, which data sources every Member State will provide, and which agencies are charged with collecting it. This development cycle includes procurement, and because states initiate these projects at different points in time, it is often difficult to coordinate procurement initiatives.

Even if not embedded into the policy cycle, but being equidistant from policy, end-users and market stakeholders, standards organisations were also brought into the picture.

- **CEN & CENELEC**. CEN & CENELEC catalyse business in Europe by removing trade barrier for European industry and consumers through the development of standards. It is a network of more than 2000 experts. CEN & CENELEC define a standard as a reference document that sets out technical specifications and that sets out the minimum requirements on the quality and/or performance on a product of service. Standards are developed with input from industry, consumer representatives, and SMEs. All standards are consensus based, which means that all committee members agree to implement them once they are established. Standards **improve efficiency of key processes, facilitate systems integration and interoperability, and enable the drawing of comparisons between products**. This allows users to better assess new products or services, structures the approach to developing new technologies and/or business models, and generally has the benefit of simplifying complex environments.

Research

Stakeholders within the research category play (as outlined in previous paragraphs) an important role in informing the decisions of policymakers as they relate to information exchange and interoperability.

Relevant projects and project outputs

Activities conducted as part of the following projects and/or organisations were outlined during the 11th CoU meeting:

- **DRIVER+**. DRIVER+ is about supporting practitioners in their own capability development, further stimulating innovation in crisis management (CM), improving practitioner involvement, increasing business opportunities for industry, and sustaining and further developing project results. The project's concrete outputs consist of a pan-European Test-bed for CM capability development, a comprehensive portfolio of crisis management solutions, and a shared understanding of CM across Europe. As part of the test bed program, DRIVER+ provides a support structure to guide potential users which consists of a trial guidance methodology and of support training. As the project's deliverables have recently been greenlighted for publication by the Commission, several of the projects outputs (notably, the back-end code of the testbed) are – as of recently – publicly available through GitHub.
- **ISITEP**. ISITEP is geared, first and foremost, towards researching how interoperability can be ensured within EU

project by design. EU security threats are increasingly not only external, but also internal. Closer cooperation between EU states represents the clearest solution to challenges such as terrorism. In order to implement interoperability, all spectrums - from technical to legal/political - need to be corrected for. With this in mind, the project ensures that a bottom-up as well as a top-down dialogue is present between the various stakeholder categories. The project's main outcomes are comprised of a.) network solutions (ISI gateways) and radio terminals, b.) a study on procedures, based on the legal and procedural standpoints outlined within a case of Norway-Sweden, and c.) uniform communication standards and infrastructure. The network standards developed by ISITEP have already been adopted by Norway and Sweden. Luxembourg, Belgium, Finland, and the Netherlands are likely to follow suit.

- **ALFA**. The ALFA project is geared towards identifying and tracking the low-flying aircrafts which are often used to ferry contraband products (drugs, etc.) across EU borders within the Strait of Gibraltar. In practical terms, this means it tracks everything from airplanes to drones. Tracking these vehicles constitutes not only a technical and operational problem (which systems can track them, how can false alarms be avoided, etc.), but – because Spain and Portugal are both affected – also a transactional problem. Project ALFA's solution allows these countries to combine geographical, radar, and optical (video)-based data with detection and classification techniques to identify likely landing areas on the basis of flight path analysis. In order to overcome interoperability issues between practitioner groups, the project streams results to a smartphone app that can be used by any eligible user.
- **ROBORDER**. ROBORDER is an H2020 Security project with over 20 partner organisations (10 of which are practitioner groups). The project provides autonomous border surveillance. This requires merging static systems (such as radar) with autonomous systems. In a perfect world, unmanned aerial vehicles (UAVs) coming from manufacturer A can share data with a radar build by manufacturer B. But this is hardly ever the case in practice. As threats and technologies change, the nature of interoperability will need to evolve over time. ROBORDER is based on the premise that, as the world (and practitioner budgets) shrink, the need to make smarter use of existing systems through interoperability is increasing. ROBORDER places great stock in the value of ensuring that all stakeholders feel comfortable with standards and common practices. It achieves this through the provision of a user interface (UI) to which legacy surveillance systems can easily connect and through adherence to a NATO-developed data input model. This has helped the project to gain the critical user mass it needs to remain operational.
- **INACHUS**. INACHUS tries to identity victims within rubble in urban environments. Interoperability encompasses organizational and technical domains, and these need to push one-another to reach a viable outcome. INACHUS works with technical tools to facilitate rich information exchange during the response phase of a disaster. This includes the development of modular robots and a software tool which visualises a common operational picture. Responders often have simulations to work with when identifying victims on-scene, but these can be complemented by a wide range of other technical (including UAVs with head sensors, mobile antennas, etc.). In order to yield actionable information, these tools need to be able to exchange information with one-another. In the project's final phase, the INACHUS is pushing for standards and for widespread adoption.

In addition to the previously outlined projects, the **Broadway** and **Broadmap** projects were also touched on and/or shortly discussed during the the 11th CoU meeting. The Broadway and Broadmap projects are a pre-commercial procurement project and a preparatory action, respectively, geared towards facilitating the eventual procurement of an EU-wide broadband communications network. Other relevant projects include **ATHENA, EMYNOS, NEXES, ATHENA, IN-PREP, SLANDAIL, HEIMDALL, SECTOR**, and **IsitEthical**.

Possible synergies (and links to policies and practitioners' operations)

Within the field of interoperability, there are clear synergies between research outputs, practitioner needs, policymaker initiatives, and industry activities. Initiatives such as the International Forum to Advance First Responder Innovation (IFAFRI) – currently chaired by the European Commission's DG HOME – show clearly how research activities can bridge the gap between practitioner needs, limited policymaker knowledge, and industry activities, thus leading to common interoperable solutions.

Embedding research into a wider capability development process can also contribute to better streamlining the common needs of EU security practitioners and to developing innovative solutions which not only are interoperable by design, but which are also triggered by policy priorities, respond to critical and urgent operational needs, and show an adequate balance between cost and effectiveness.

For an overview of information exchange and interoperability-related projects funded under the Horizon 2020 framework prior to 2016, see section 9 (Horizontal issues) of **DG HOME, "Community of Users on Secure, Safe and Resilient Societies - Mapping H2020 and ISF Projects Funded under 2014-2015 Programmes," Working Paper (Brussels: European Commission, forthcoming**). The projects referenced within this section of the aforementioned document are universally geared towards tackling similar subjects as those discussed in this brief, and thus have the potential of exhibiting synergies with them.

Lessons learnt and challenges

Despite the clear benefits associated with realising such an outcome, several phenomena impede progress towards 'perfect' information exchange and interoperability between stakeholders within the field of security at the European level. With regards to transactional barriers to information exchange and interoperability, these relate almost entirely to the fact that stakeholders are sometimes reluctant to share information with other organisations as a result of a lack of organisational familiarity (read: trust). At the level of the EU public sector, this problem is compounded by linguistic and/or cultural barriers, which further complicate the prospect of building repertoires between organisations. The challenges observed within the EU public sector are partially mirrored within the private sector, which is increasingly comprised of organisations (insurance firms, social media giants, hardware manufacturers) which preside over information that has utility from the first responder perspective. In forging productive relationships with these actors, security end-user organisations must increasingly learn to navigate an environment which features not only institutional non-familiarity, but also privacy concerns and vested financial interests. With regards to the vested financial interests of private sector organisations as they relate to interoperability, it pays to note that interoperability can (depending on perspective) simultaneously offer financial opportunities and pose threats. Just as technology giants such as Apple and Google go to great lengths to 'lock' consumers into their respective ecosystems by pursuing 'non-interoperability by design,' firms which supply end-users with technology have an incentive to pursue customer and/or market monopoly through the introduction of proprietary standards.

Technical challenges can be generalised as resulting in end-users either a.) not being able to receive data, b.) not receiving data in a timely manner (meaning that the data cannot be transposed into actionable information), or c.) not being able to process received data. Though the causes of technical interoperability vary by the type of system and/or data in question, its costs can be summarised as taking the form of more costly procurement cycles, less adaptable organisations, and reduced operational agility.

Transactional and technical barriers to 'perfect' information exchange and interoperability can be addressed through a combination of top-down and bottom-up initiatives. These are further discussed in the **Way forward** section.

Way forward

Experience gleaned from (among others) the H2020-funded **FIRE-IN** project indicates that no 'quick' solution exists for addressing transactional barriers to interoperability, and that bottom-up initiatives to alleviate the phenomenon should ideally be coupled with top-down measures. With regards bottom-up initiatives, these present in the form of the organisation of focused events which facilitate the process of a.) building relationships between organisations, and b.) fostering shared organisational understanding regarding the utility and expected use case and/or handling of the to-be shared data. Top-down measures include (among others) the communication of political will through the signing of 'trailblazing' bilateral (or multilateral) agreements and the adoption of legal frameworks which facilitate information sharing between organisations by clearly stipulating the consequences associated with utilizing information to further goals which fall outside of interagency agreements. The introduction of such a legal framework also serves to alleviate challenges associated with concerns regarding user privacy within the private sector.

To prevent a scenario in which a single supplier fosters widespread dependence through the introduction of a non-interoperable standard, policymakers should strive to introduce (and foster acceptance for) well-informed standards of their own. In order to ensure these standards' success, policymakers should enlist researchers to formulate standards which are compatible with existing platforms, are simpler to adhere to than they are to diverge from, and are field-validated. Standards which exhibit these characteristics tick all the boxes associated with realising critical user mass and are therefore well-equipped to succeed. Policymakers can further foster a critical user mass for an agreed-upon standard by enforcing its inception throughout procurement processes, from pre-commercial to commercial. Because it can take EU legislators between 25 and 35 months to agree on a standard (a period which is considerably longer than most EU-funded projects), consensus between stakeholders (policymakers, practitioners, and industry & SMEs) is key to ensuring that the outputs of past projects – and the lessons learnt throughout their development – can feed into the process of streamlining future procurement cycles.

Though the aforementioned combination actions should resolve the majority of barriers to information exchange and interoperability, end-user organisations may still face technical barriers which derive from a lack of in-house capacity to implement changes which accommodate new standards and/or modular technologies.

Key Contacts

CoU website:
http://www.securityresearch-cou.eu/

EC DG HOME
Philippe Quevauviller
Philippe.Quevauviller@ec.europa.eu
David Rios-Morentin
David.RIOS-MORENTIN@ec.europa.eu

DRIVER+
http://www.driver-project.eu
Peter Petiet
coordination@projectdriver.eu

ISITEP
http://isitep.eu/about/
Federico Frosali

ALFA
Project website
Rob van Heijster
rob.vanheijster@tno.nl

ROBORDER
http://roborder.eu
Andre Oliviera
andre.oliviera@tekever.com

INACHUS
www.inachus.eu
Evangelos Sdongos
Evangelos.sdongos@iccs.gr

EUCISE 2020
http://www.eucise2020.eu/contacts
Emanuele Bellini
emanuele.bellini@unifi.it

Related readings / publications

- J. E. Bruzdzinski, J. Selby, and A. Tolk: Challenges to Modern Allied Force Acquisition, Integration, and Interoperability; MITRE Report, 2018, Released for unlimited distribution (Case-No. 18-1151).
- J. Selby, and A. Tolk: Interoperability Readiness Levels in Support of Operational Agility; MITRE Presentation, 2018, Released for unlimited distribution (Case-No. 17-3081-11).
- New European Interoperability Framework: Promoting seamless services and data flows for European public administrations, © European Union, 2017, SBN 978-92-79-63756-8.
- European Union: European Commission, Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: European Interoperability Framework – Implementation Strategy, 23 March 2017, COM(2017) 134.
- European Union: Factsheet, Interoperability of EU Information systems.
- European Union: European Commission, Communication from the Commission to the European Parliament and the Council: Stronger and Smarter Information Systems for Borders and Security, 6 April 2016, COM(2016) 205.
- European Union: European Commission, Communication from the Commission to the European Parliament, the European Council and the Council: Seventh progress report towards an effective and genuine Security Union, 16 May 2017, COM(2017) 261

Forthcoming CoU events & other related events

- 12th CoU Meeting, 3 – 4 December 2018, Brussels
- Security Research Event (SRE) 2018, 5 – 6 December 2018, Brussels
- International Forum to Advance First Responder Innovation, 5 – 7 December 2018, Brussels

European Commission