Reviewed by Edoardo Del Principe, Research Assistant 2020, U K Defence Forum

European documents between agenda-setting and real strategy

The European Commission recently set out a new EU Security Union Strategy (ESUS) for the 2020-2025 period. The document updates the previous security agenda of 2015-2020 , reprising cardinal points and adding depth to the European strategy. It is not the first time the word "strategy" appears in a European document; perhaps the most famous was in the European Global Strategy.

Such material can sound maybe generalist or vague, but this is an inner weakness of every "grand-agenda," which cannot cover every aspect in depth. It could be inappropriate to use the word "strategy": such documents usually set policy guidelines for future politics. However, in this case the ESUS has a little bit more of a strategic flavour.

While the EUGS is a more an "agenda-setting" document, the ESUS establishes priorities and propose actions. It is for one primary reason: the EU has not the power to set its foreign politics autonomously without the approval of the 27; it can only put guidelines on the table. In the ESUS, there are references to new or pre-existing European agencies, legislative proposals, and a cause-effect relation between policy and the expected results. Anyway, without the good faith and effort of the 27, this strategy could not be decisive.

Part of the document bases its action on legislative modifications that the EU proposes, and the Member States must accept and apply in their law. Especially in the cyber domain, where there is still a significant distinction between offline and online crimes, States are expecting to promote new modern and efficient regulations. The document underlines the cause-effect relations between lack of normative and increasing crimes or fragile infrastructures and vulnerable systems, and it proposes actions in bullet points at the end of every part.

Even if the EU has not all the tools to create by itself a "security ecosystem" as described in the document, the bullet point proposals could help in the reception of the paper as not only a top-down policy proposal but also as a useful guide to face current problems.

What is a "security ecosystem"?

The EU has been trying in recent years to have a more global approach to issues, a 360 view that could help legislators as well as technicians to define and pursue policies more effectively. The Union differentiates between "cooperation" and "information," as the fundamental assets of its strategic ecosystem. It means that member states are expecting to cooperate at a higher level within the Schengen Information System framework. Member states should have a policy harmonization process to implement European directives on cybercrime, data sharing, and human rights violations to reduce fragmentation and upgrade available instruments. On the other hand, the EU is expecting to give more incentives to develop new technology in the security field and to use existing tools like the EU INCENT, Europol, and Eurojust "to maximize the synergy between law enforcement cooperation and judicial cooperation." In brief, a security ecosystem is a framework where multiple actors cooperate to maintain a safe physical and digital environment with data sharing and using collaborative tools.

Weak infrastructures and vulnerable systems

One of the main points expressed in the document is the relation between weak infrastructures and vulnerable systems. The ESUS outlines that there is no significant distinction between physical/digital crimes because, nowadays, the implications in one domain have effects on the other, making it impossible to separate the two worlds. It is wrong to perceive the online realm as not physical when its whole infrastructure is.

On the other hand, every physical infrastructure depends on systems that are often entirely digital, relying to work on the operability of these digital systems. Because of this, the EU wants to improve resilience in the cyber sphere through a culture of cybersecurity by design, "with security built into products and services from the start". The Union emphasises the importance of future G5 infrastructure. It warns on the inter-dependence of all the services that use the network, meaning that any possible attack or disruption could cause a snowball effect on services. The Commission identifies the need for a Joint Cyber Unite to provide a higher level of coordination and cooperation between EU institutions, bodies, and agencies.

Protection of public spaces is also essential. Places of worship, transport hubs, or anywhere else open and accessible have been the target for terrorist attacks. The Commission hopes for more cooperation between the public and private sectors through better regulation and more money invested in the safety of these shared places. The first to be protected should be minorities or any discriminated portion of society.

The relation between security and freedom

This new security strategy does not contrast security with freedom. Instead, it says that freedom depends on the level of protection we have. However, any high level of security means more control over our actions, behaviours, technological systems, and information-sharing programs . It is something that has not been taken into consideration by the documents and something that must be discussed to avoid restrictions and punitive law reformation in the name of more security. The word "terrorist" is used to identify organized groups as well as political opponents. The concept has many definitions; because of this, any law enforcement on this field must be meticulous. As Benjamin Franklin once said "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."
.
Freedom is not something that we estimate with a measuring stick; people perceive freedom, and a higher level of security and control could threats this perception. Instead, security is in a certain way measurable by the strength of our systems to fight cyberattacks or by the level of protection of our physical/digital infrastructures

It is a tricky field because you can measure this kind of policy by its effectiveness, but it is often quite impossible to predict its impact of society. If any member states are autonomous in the definition of these new practices in its law code, without any surveillance by the Commission, there could be serious and permanent impacts.