Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Departement of Justice and Police FDJP

Federal Office of Police fedpol
International Police Cooperation
Division Strategy

Consultation on the renewal of the EU Internal Security Strategy

Contribution of the Federal Office of Police fedpol, Switzerland

1 General Remarks

Innovations in information communication technologies have increased the possibilities for free exchange and the unhindered exercise of the right to freedom of expression and information. At the same time, they have increased the capacity of States and non-State actors to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy. To be acceptable from a human rights standpoint, all forms of restrictions must have a legal basis, clearly be in the public interest and respect the principle of proportionality.

2 Which specific challenges need to be tackled by EU action in the coming five years regarding international crime, radicalisation and terrorism, cybercrime and cyber-attacks, natural and man-made disasters? What role should the border security have in addressing those challenges?

2.1 International Crime

2.1.1 Human trafficking and Human smuggling

Trafficking in human beings is a serious crime and violation of human rights, which can be classified as a modern form of slavery. It occurs all over the world and affects almost every country as an origin, transit or destination country or sometimes a combination of all.
The global scale of human trafficking is difficult to quantify, due to the hidden nature of the crime. Figures often may have been based on conflicting definitions or compiled for different purposes, and are therefore seldom comparable. Trafficking in human beings is often linked with other forms of organised crime.
Human trafficking takes place in secret and can't be determined without further notice. The perpetrators operate with much effort to disguise exploitation situations and present them as something else. Special knowledge about this type of crime is necessary for the recognition

of human trafficking and victim identification.
There are many reasons why victims exploited by the occasion of milieu controls don't want to portray their hopeless situation versus the police or in a proceeding to law enforcement authorities: The perpetrators intimidate the victim. The forms of psychological and physical violence and threats are very varied and often very subtle, consider cultural backgrounds, and are not identifiable for the authorities right away. The most effective threat is that something will happen to the families in the country of origin if the victim will not meet the expectations of the offender. It may be that the victims begin to identify with the objectives of the perpetrators as a result of coping with their situation or it can come to personal level relationships between perpetrators and victims.
Despite existing efforts it comes to relatively small numbers of condemnation in the suspected extent.
Reasons for the recruitment of always new victims could be the increase in migration, also within Europe.

2.1.2 Person identification misinterpretation

The person identification for law enforcement applications based on biometric means, namely fingerprints, is widely used and established. The current development in this area is characterized by a sequential check of fingerprints against an increasing number of fingerprint databases: national automatic fingerprint information system (AFIS), Prüm, VIS, Eurodac. The requesting agency receives individual results of every request at different points in time. This can lead to unnecessary collection and misinterpretation of results, and it is absorbing man-power.

2.1.3 The Role of the Border Security

Border security has an important role. Border authorities should have access to all the available information like the Interpol database for lost and stolen travel documents (ASF-SLTD), SIS, VIS, ICAO Public Key Directory (ICAO-PKD) and other information system with one only query of their system. Automation in border controls should be enhanced to free resources that can be used in other areas (like manned border patrols etc.).

2.2 Radicalisation and terrorism

2.2.1 Major transnational security challenges

Major transnational security challenge(s) to Western (and Central) Europe in relation to jihadist terrorism and extremism in the next five years:

- Battle-hardened foreign terrorist fighters returning to Western Europe after having joined a jihadist or other armed group in the Syria-Iraq region and the military-style training (as illustrated by the small-arms attack on the Belgian Jewish museum in Brussels on 24 May 2014);
- Continued terrorist and lethal tactics in insurrectionist anarchism, namely in the Mediterranean, employing both improvised explosive and incendiary devices (IED/IIE). Some of these networks are also linked to like-minded present in Switzerland or capable to pass to action either on Swiss territory or against Swiss interests abroad;
- Massive, highly sophisticated and effective misuse of social internet media for terrorist purposes, as illustrated by the current, unprecedented propaganda campaign by the "Islamic State" in the Syria-Iraq region and its supporters;

- Potential proxy conflicts between supporters of the “Islamic State” and its victims/adversaries in the Syria-Iraq region (e.g. between Europe-based violent Salafists and Kurdish groups).
- While speaking of foreign fighters, the first thought is about Islamic extremism. But we should not forget other forms of foreign fighters, for example those with nationalistic background.

2.2.2 Role of the border security in addressing those challenges

- Early detection of battle-hardened foreign terrorist fighters is needed in the process of returning or about to return to the Schengen area and timely information exchange between concerned member states, including Switzerland;
- Systematic and proactive information exchange on such returned foreign terrorist fighters (once they are inside the Schengen area) as well as on Syria-/Iraq-bound foreign fighters (i.e. those that have not yet travelled to the region, but are intent on or in the process of doing so);
- Systematic and proactive information exchange on insurrectionist anarchist individuals, networks and activities inside the Schengen area;
- Permanent support (know-how, instruments) in recognition and detection of ID and forged documents and the recognition of Impostors in the context of border controls and, increasingly, at police motivated checks within the country.

Effectively countering the social media abuse for terrorist purposes has to become a top priority.

2.3 Cybercrime/Cyber-attacks

2.3.1 Developments in technology

Technical developments in the next five years might exacerbate existing security challenges and create new ones. Firstly, with targeted advertising as one of the major sources of income for the biggest internet service companies, the exchange and algorithmic processing of user provided personal data in order to generate the most revenue out of targeted advertising is becoming one of the main thriving economic concepts of the internet. This leads to a centralization of personal data, which in turn produces challenges for data protection and privacy while increasing the adverse impact of potential data loss, theft or leakage. Secondly, anonymization services and networks are experiencing a growth of their user base. The abuse of such networks for criminal activities is also growing. Due to the nature of such technical networks that try to heavily reduce the traceability of a user’s online activities and to mask its geographic location, law enforcement is heavily challenged through jurisdictional issues. Finally, control systems, both consumer and industrial grade, are becoming much more connected via the internet, due to the convenience of being able to remotely control even the most complex systems and let those systems communicate with each other automatically in order to gain maximal efficiency. This development leads to new possibilities for attackers to exploit security gaps and get direct access to home or corporate networks.

2.3.2 Law enforcement challenges

The ever increasing coupling of the financial real world identity of an individual with his or her digital entity creates more opportunities for identity theft. As recent password leaks and account hackings show, data theft and subsequent abuse of the acquired data, e.g. in credit card fraud, is a thriving business in the underground economy. As the importance of an individual’s digital identity is evolving around social media profiles / email addresses / username-

password combinations, ever more services on the internet use these profiles as a means of authentication in order to process payments via payment methods that are associated with those identifiers. Therefore, ever more potential opportunities for cyber criminals to monetize stolen account information are created.
The digital identity is generally not bound to a geographical location but can be accessed from any place on the world within microseconds. However, the action radius of law enforcement agencies is primarily restricted to their own territory, or slowed down by non-existent or often time consuming mutual legal assistance procedures.
Legal issues about liability in cases of data theft may arise, as laws of EU member states may conflict with the laws of the countries the web services are located in.
The business model «Cybercrime as a Service» leads to ever more sophistication of attack methods as well as coordination of attacks against institutions or individuals. In Switzerland, an increase of sophistication in Spam / Phishing emails as well as telephone calls or organization of money laundering schemes that launder profits from attacks against e-banking systems is observed. Already now, for untrained users it is very hard to distinguish between legitimate business emails and phishing mails for certain types of attack. It is expected that the increase in sophistication and coordination will continue on in the next years.
Individuals will thus continue experiencing widespread untargeted attacks in order to get access to their sensitive data. Actors in the underground economy will continue to find ways to exploit security gaps. From classical phishing emails for credit card information to stealing personal data stored on communication devices, there are numerous ways cybercriminals can benefit from executing attacks against the ever increasing multitude of devices. The high number of potential victims that are targeted with one single attack wave is what makes them financially lucrative.

2.3.3 Particular challenges for critical infrastructure

Cyber attacks on critical infrastructure can have particularly severe consequences, as they can compromise vitally important functions or trigger fatal chain reactions. Therefore, (often private) Critical Infrastructure operators play a key role as providers of important services with overriding security implications. Attacks against critical infrastructure, both industrial and government, have shown that even complete separation from the internet is not a guarantee that attackers will not get access to critical infrastructure controls. These often state sponsored and tailored attacks are generally very hard to detect since the means used are heavily customized to the attacked systems and designed to be stealthy in the first place. With ever more critical control systems of industry and government installations connected in some way or another to the internet, the number of possible targets for industrial or state sponsored sabotage is increasing. This poses a security risk with potentially dramatic economic as well as political impact. Also, to detect and trace attacks on critical infrastructure requires a high degree of knowledge and specialized skill, as well as very specialized forensic equipment. The prosecution of state sponsored attacks has been proven very difficult, also due to political and jurisdictional reasons.

2.4 Protection of critical infrastructures

Critical infrastructures ensure the supply of essential goods and services such as energy, communication, or transport. Large-scale failures have serious consequences for the population and the economy. They also have detrimental effects for the security and welfare of the state. Until now, severe failures have been rare and of short duration. However, due to the proliferation of new – and sometimes not mature – technology and to globalization, the importance of critical infrastructures has vastly increased. A large-scale power blackout, for instance, could paralyze the economy of large parts of Europe and would cause outages in the other critical infrastructures (e.g., telecommunications, water supply, or rail transport),

and would also severely affect the population. Also, the nature of risks has changed and continues to change in the coming years: for instance due to the effects of climate change, malicious physical and cyber attacks, or aging infrastructure. Furthermore, in the case of an adverse event, the strong interdependencies require increased collaboration of all actors across the various critical infrastructure sectors within and across countries.

3 Taking into account the developments in the next five years, which are the actions to be launched at the EU level?

3.1 Protection of victims of Human trafficking and Human smuggling

During a control, it would be wrong to exclude the existence of situations of exploitation because of the first statements of the victim. Rather, further ongoing investigations in the operation must be made.
There are more efforts needed in the areas of prevention, prosecution, protection of victims and cooperation at European and international level - with governmental and non-governmental organizations.

3.2 Actions against cybercrime/cyber-attacks

One of the major contributing factors to the underground economy is the slow response from law enforcement authorities investigating data breaches and thefts in comparison with the time it takes for the perpetrators to transfer the stolen data outside of the respective jurisdictions. Given the transnational nature of cybercrime, cooperation among law enforcement authorities at the EU level and beyond is key in fighting cybercrime. Legal and non-legal frameworks that facilitate cooperation and reduce response times should thus be enhanced and developed. Strengthening the roles of coordinating authorities such as Europol in order to perform more efficient and coordinated action could be one way forward in tackling these challenges.

Similarly, legislative issues for data protection and privacy may become a problem where a solution on the level of the individual member states will be no longer practical. Instead they will need to be resolved on a pan-European or even global level.

With ever more services available, it will become even more difficult for law enforcement to keep up with the technological challenges. Private-Public-Partnership is crucial for developing meaningful solutions. Especially, partnerships have to be sought with providers of financial services in order to investigate cases of money laundering or short response time interception of illicit payments. Similarly, close partnership with critical infrastructure providers are key.

3.3 Actions against data leakage of EU systems

The successful implementation of the already existing technologies requires significant preparation and careful ongoing maintenance. For this reason, it is important to exchange our

knowledge and to find a common solution. Regarding the data leakage prevention, this issue should be intensely discussed and a solution with significant effort should be prepared to greatly reduce risk to the organization. This implementation solution should have a strategic approach that takes into consideration the risks, the impacts and the mitigation steps, along with appropriate governance and assurance measures.

3.4 Actions against person identification misinterpretation

In order to streamline this process for the sake of efficiency and error-resistance, it would be important to investigate the possibilities in legal, technical and process-oriented aspects.

3.5 Border controls

Strengthen and harmonize border controls at all external borders, including airports. Taking into account the availability of eMRTDs (Electronic Machine Readable Travel Documents, also called biometric passports) and biometric Visas, binding standards for checking these documents should be established and audited. This would also include the mandatory use of the available information from information systems like SIS, VIS, ASF-SLTD, ICAO-PKD etc. Allow for law enforcement access to data in the future Entry-/Exit-System (EES). However, one of the main challenges is interoperability between existing and future information systems allowing for a smooth and risk oriented border control process in view of a rising number of travellers.
Furthermore, in order to fight the human smuggling and human trafficking, the cooperation with third countries and transit countries must be encouraged in order to cope with the increasing illegal migration.

The protection of external borders is of particular importance for the safeguarding of internal security in the Schengen States. The external border controls are therefore continually improved (SIS II, VIS, EES, etc.). The use of biometric data (fingerprints, facial images, etc.) is becoming increasingly important and this should be encouraged, because such data allow a precise identification of persons, which is also used to fight terrorism.
In addition, the detection of forged or falsified documents plays an important role in the fight against terrorism. Another prerequisite is the timely exchange of information and the creation of common risk assessments. Another is to promote close cooperation between all national border control authorities among themselves (border police, customs, border guards, etc.).
With the increasing mobility of persons and goods, States need to address the challenge of ensuring the right balance between open, but at the same time secured and controlled borders. In order to respond to this challenge, the European Union (EU) has developed the concept of “Integrated Border Management” which is the key to the European border management strategy. The idea of the integrated border management should be consistently lived and implemented on Schengen level and at the level of each Member State. Access to Eurodac for law enforcement agencies and the "Smart Borders" package should also be promoted. Instead of new measures, existing measures should be applied consistently and should only be extended if they result in operational added value.

4 Which specific research, technology and innovation initiatives are needed to strengthen the EU´s capabilities to address security challenges?

4.1 Research

In order to assess the situation in the dark net as well as get an accurate estimate on the criminal revenue that is generated out of the abuse, both for distributing Child Sexual Exploitation material (CSEM) as well as in the trade with illicit goods, it is suggested that coordinated international studies, both by law enforcement authorities and independent research institutes are performed.

Especially, we suggest that research is performed in the following issues:

- Specific tools (search and indexing in the dark web)
- Legal and technical issues in surveillance software
- Traceability of alternate currencies
- Development of image and victim identifying software: PhotoDNA…
- Development of cryptography tools to counter cryptographic forensic countermeasures

4.2 Technology

Currently the EU disposes of many different and good technologies to address security challenges (i. e. for border controls), but they must be deployed and operated correctly to maximize the benefit of these technologies. The focus should therefore be on the deployment, training and use of available new technologies.