PUBLIC-PRIVATE PARTNERSHIPS IN CYBERSECURITY

BRIEF

As we become more and more digitally active, the security landscape follows suit. Over the last years we have seen a fundamental shift in the nature of security threats from the traditional spheres to cyberspace. This development asks for new approaches to deal with these threats. A recent initiative at the European level is the launch of public-private partnerships for cyber security. In this policy paper we will discuss this initiative and its place in a changing security environment. Why are they necessary? What are the benefits? And how can they contribute to better cyber resilience?

The experts mostly agree that the next big conflicts will most likely take place in cyberspace. This was exemplified at a major event organised by 'Friends of Europe' entitled 'Security Jam 2016' which saw over 2000 people in attendance, among which leading experts in the field of security. When asked to identify what dimension of the battlefield the most powerful nation in the world in 2030 would control, 52 % of them chose 'Cyberspace'. The options were the traditional military areas; land, sea, air and space, and cyberspace.

The rising threat of cyberattacks is not confined to the military domain alone. Businesses and consumers are equally at risk. According to a recent survey, the number of security incidents across all industries rose by 38 % in 2015 and more than 80 % of European companies have experienced at least one cybersecurity incident over the last year.

When it comes to remaining in control over cyber space, the most important word is *resilience*. By resilience we mean the ability to anticipate, absorb, adapt to and rapidly recover from disruption caused by a cyber attack. This requires the systematic implementation of preventative, detective, and reactive measures to ensure that organisations can continue their operations during and after attacks.

Achieving resilience in cyberspace requires a healthy and active public-private partnership. In 2011 the European Union Agency for Network and Information Security (ENISA) published a report on good practices in cyber security PPPs. According to this report cooperation between the public and private sector on cyber security is necessary because the public sector is responsible for national security while the private sector owns most of the infrastructure that needs to be secured.

Additionally, cyber threats have developed to a level of sophistication where very few or none can withstand them on their own. Therefore, it is crucial that governments and businesses pool their knowledge,

information and expertise to develop a strategic approach to research and innovation. This of course requires more public funding, but it is also essential that the private sector sees the need to invest in these capacities themselves.

Cooperation between the public and private sector can bring benefits for both sides. For the public sector a PPP can be a solution for a lack of funds or a lack of capabilities. For example, it can be too expensive to involve all SMEs in a national strategy fully covered by the national budget. Working in a PPP allows the government to cooperate with the private sector in a way that it is worthwhile for companies to invest their own money. For the private sector a PPP offers a way to address problems that go beyond the boundaries of single companies or industries. Moreover, it can also be a way for the private sector to have influence on the national security strategy.

A vast majority of today's E-services offered by the European governments are in fact provided by private companies, and these services are very likely to increase dramatically over the next ten years. So too are the threats and intrusions facing them from both state- and non-state actors in terms of cyber-attacks that could cripple these services.

This spring the European Liberal Forum held a high-level roundtable discussion on the fringes of the *Munich Security Conference* (MSC) on the subject. The panelist all agreed that it is of crucial importance that governments do not stall the evolution of public-private partnerships. Instead, they should make sure that companies are encouraged (and sometimes demanded) to communicate with each other and with governments, and share information on possible intrusions in their systems. The coming into force of the NIS Directive (on security of network and information systems) in August 2016 is a step in the right direction. With the legal framework in place, it is now important to nurture industrial capabilities and to stimulate their implementation by companies, public authorities, and citizens.

It is also important that governments offer action plans for tackling cyber offences directed against its contractors.

It is not only the E-services provided for citizens that are often in the hands of private companies, today a vast part of our *critical infrastructure* is owned, or supported, by private actors, like the telecom networks or our railroads. Since these areas include a clear national security priority it seems only natural that governments partner with companies in the planning of securing this infrastructure, and involve them in the *civil-emergency planning* and have them in from the start in the civil preparedness plans for securing such infrastructure. This should be done in such a way that authorities do not become too dependent on any single private actor.

Another group that is easily forgotten in the cyber security debate at a state level are the consumers. Consumers in the digital market want innovative products that work, and deliver their needs, regardless of who the provider is, and regardless of where that provider is based. This means that if Europe does not want to lose business to providers based elsewhere we have to make sure that our standards are easy to understand and that a dialogue is maintained with the service providers. Which means standardisation and demands cannot be to too complex, and must take the business in consideration.

This means that cyber security has an essential role in the formation of the 'Digital Single Market' in Europe, and within that framework there needs to be a working dialogue and trust between the public- and the private sector. This trust does not only lie in having guidelines for sharing information on security strategies but also in making clear rules for *data protection*, rules which would cover issues such as when companies are required to hand over consumer data to governments, and what data governments can let private actors analyse.

Liberal Commission Vice-President in charge of the Digital Single market, Andrus Ansip, said this summer that "Without trust and security, there can be no Digital Single Market. Europe has to be ready to tackle cyber-threats

that are increasingly sophisticated and do not recognise borders. Today, we are proposing concrete measures to strengthen Europe's resilience against such attacks and secure the capacity needed for building and expanding our digital economy" as he launched a new investment plan to strengthen the partnership between the public- and private sector on cyber security.

The Commissions investment plan is bold; it is investing €450 million in this partnership, which is expected to trigger € 1,8 billion in investments by 2020. These funds will be used to create joint projects between the European Commission and cybersecurity market players, represented by the European Cyber Security Organisation (ECSO). Also included in the partnership are members from national, regional and local public administrations, research centres and academia. The investments are welcomed by liberal groups as they go into research and development to ensure that key knowledge in this field is developed, and kept, in Europe.

The aim of the investment plan is twofold. On the one hand, it should make European cyber security businesses competitive on the global market. On the other hand, it should secure that Europe has access to state-of-the-art cyber security technologies. This combination of security interests and economic interests is a distinct liberal position and is certainly a positive development.

KEY SUGGESTIONS FOR ACHIEVING BETTER RESILIENCE IN THE FACE OF CYBERATTACKS:

- Raising awareness about cyber threats, both with companies and with private consumers, and training and educating small- and medium size enterprises in cyber security.
- Streamlining communication between governments and big actors on the digital market.
- Larger involvement of private companies in civil-emergency planning and making it standard to include them in those exercises.
- Better harmonisation on cybercrime legislation, and streamlining law enforcement capabilities in the EU.
- Speedy and efficient implementation of the NIS Directive to create legal certainty.
- Putting extra effort into teaching (and hiring) the next generation of cyber experts.
- The European states need to find a way to not only delegate authority to the public sector in these matters, but also to delegate responsibility to national security – trust is the key word when it comes to the public- private partnership in this field.
- It is vital that the EU speaks 'with one voice' at the GGE (UN Working Group of Governmental Experts on Developments in the field of Information and Telecommunications in the Context of International Security) when discussing future international cooperation on cyber security.

AUTHOR
BJÖRN BONSDORFF | RESEARCH ASSOCIATE, EUROPEAN LIBERAL FORUM

Co-funded by the European Parliament. Neither the European Parliament nor the European Liberal Forum asbl are responsible for the content of this publication, or for any use that may be made of it. The views expressed herein are those of the author(s) alone. These views do not necessary reflect those of the European Parliament and/or the European Liberal Forum asbl.