



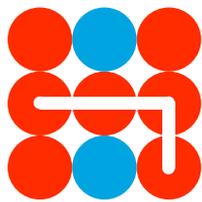
---

Strategic Analysis March 2018

**Countering Hybrid Threats:  
Role of Private Sector  
Increasingly Important.  
Shared Responsibility Needed**

---

JARNO LIMNÉLL



Hybrid CoE

# Countering Hybrid Threats: Role of Private Sector Increasingly Important. Shared Responsibility Needed

*Cooperation between industry and governmental agencies on joint security initiatives can leverage the unique yet complementary strengths of both sectors, writes Jarno Limnéll, Professor of Cybersecurity at Aalto University, Finland, and Adjunct Professor at the University of Jyväskylä, the Finnish National Defence University, and Tampere University of Technology.*

It is often overlooked in security analyses that the private sector has an essential role to play in striving for security. In many Western countries, 80–90% of all critical infrastructure is owned and operated by the private sector. **The first line of defence often resides outside of the government and lands squarely on the shoulders of private industry. It is important to protect critical infrastructures (e.g. energy supply chains, transport, public health), since an unconventional attack by perpetrators of hybrid threats against any “soft target” could lead to serious economic or societal disruption.** Particularly when securing a nation’s critical infrastructure and developing its resilience, shared responsibility between the public and the private sectors is a necessity. This must take into account the fact that the public and private sectors alike can benefit

from working together. Cooperation between industry and governmental agencies on joint security initiatives can leverage the unique yet complementary strength of both sectors.

In the age of hybrid threats, cooperation between the public and the private sectors is increasingly important. “Whole of government”, “whole of nation”, and “comprehensive security” are all principles that are heard in speeches or read in national strategies to an increasingly extent today when nation-states are preparing for hybrid threats. In short, cooperation has been understood as a matter of paramount importance. The demand for inter-agency collaboration has grown when facing security challenges, and has been identified as a necessity in order to achieve an adequate level of national security for the nation. However, cooperation between public

---

**The demand for inter-agency collaboration has grown when facing security challenges, and has been identified as a necessity in order to achieve an adequate level of national security for the nation.**

---

agencies is not enough – it should be supplemented by cooperation between the government, the private sector and civil society. In fact, collaborative thinking should extend even further today, especially when preparing for threats that are not confined to national boundaries. **A “Like-minded nations” with “like-minded global companies” cooperative approach is a prerequisite when countering modern hybrid threats.**

It is now essential to adopt a broader and deeper understanding of private sector security involvement. There are numerous examples of the ways in which the private sector has become deeply involved in providing security against diverse, complex and often transnational security risks. **They are not only protecting the vital functions of society, private companies are also taking care of border security and emergency preparedness, for example. The armed forces have also become increasingly dependent on infrastructure and assets in the private sector.** The trend in Western countries is for private companies to take on even greater responsibilities task-wise, which was previously the remit of the public sector. The role of the private sector in national security is duly increasing as a result. On the other hand, careful consideration should be given to those areas of national security and vital societal functions that would be considered “off limits” for privatization.

Cybersecurity can be described as a model example of the need for public-private cooperation. Collaboration

between the public and private sectors is necessary in order to combat growing cyber-crimes, attacks and other cyber threats in contemporary society. In the EU’s updated Cybersecurity Strategy, cooperation with the private sector is fundamental for public authorities. Given the shared responsibilities of the state, industry and society will only be successful if all players act as partners. The digital world consists of privately-owned infrastructure for the most part. **Western national cybersecurity strategies categorize cybersecurity as a “shared responsibility” with a direct or indirect emphasis on the concept of public-private partnerships, and a strategic focus on the promotion of the cybersecurity industry.**

On a national basis, public-private partnerships focus on protecting critical infrastructure, serving as a strategic signal for preparedness in national security, as well as generating a competitive advantage in economic terms. If one wants to be a credible actor in cybersecurity, a strong cybersecurity private sector is needed. One example is the contractual Public-Private Partnership (cPPP) on cybersecurity between the European Commission and the European Cybersecurity Organization (ECSO), introduced in 2016. Its main objective is to promote the status of the European Union as an independent security actor by “building a strong, resilient and globally competitive European cybersecurity industry with a strong European-based offering”.

In cybersecurity, developing partnerships between government authorities

---

**Cybersecurity can be described as a model example of the need for public-private cooperation.**

---



and infrastructure owners and operators is a way to help ensure the stability and availability of critical information and communication technologies.

**Partnership helps the government disseminate vital information about vulnerabilities and security threats, coordinate incident management, and understand the resilience of critical infrastructure. The same partnership can help industry become aware of cyber threats and vulnerabilities to which it would not normally have access, and improve industry's ability to manage risk.** This must be seen as a win-win situation.

It can be predicted that private sector companies, the owners of critical infrastructure, are going to be targeted more frequently and to fall victim to more sophisticated cyber attacks in the coming years. When it comes to hybrid influencing, private companies may be the main targets. This raises an important question about the responsibility governments have to support private companies in both political and practical ways. **Companies need to be supported, particularly if they are facing adversaries (nation-state or non-state actors) who use sophisticated attack techniques.**

---

**It has been predicted that humankind might change more in the next three decades than it has in the past three centuries – because of technology.**

---

Countering cyber threats is common ground for both the public and private sectors. However, the cooperation needs to be deepened since it is a vital issue for both sectors. The public and private sectors should share more information related to cyber threats, vulnerabilities and consequences. The sectors should also work together in order to strengthen trust among societies and to discuss contentious topics related to technical solutions, such as encryption, data access and cloud servers. Another key issue entails sharing best practices related to cybersecurity education and training of end users. The public and private sectors must also cooperate through the fostering of technology innovations and investments to meet global security challenges. Public and private sector preparedness for cyber-incident management should be trained through national/international cyber exercises, which test the preparedness required by cyber incidents.

The pace of technological advancement is faster than ever at the moment. The development we are witnessing in different disciplines is huge and the effects of technological development on societies and people's lives will be dramatic. This development also raises many questions, especially in relation to the security of people and societies, as well as to warfare and business. These questions are not easily answered, since it has been predicted that humankind might change more in the next three decades than it has in the past three centuries – because of technology. **The global growth of technological companies indicates that we are going through a technological revolution that lists keywords such as digitization, robotization, virtualization and artificial intelligence. In addition, ethical issues related to the development of technology are clearly becoming of greater relevance.** A pertinent question, for instance, concerns

how to bring greater transparency to the ever-increasing number of algorithms that affect our thinking. Or what kind of ethical rules should govern the way that self-driving cars are programmed?

**today's world.** GAF A may be redefining the very notion of governance, as well as the concepts of political, societal and even geographical organizations and structures.

---

**As technological advancements are becoming more influential and the role of private companies is increasing in both world politics and security, a culture of shared responsibility will enhance the strength of democratic states and will be a powerful tool for countering hybrid threats.**

---

In this disruptive development, the role of the private sector is both increasing and increasingly more powerful. This shifts the balance between governments and the private sector. In the field of technology – probably – the most powerful actors before too long will not be nation-states but private sector technology companies. Much of the enabling technology for the fourth industrial revolution is originated, developed and exchanged in the private sector, where research and development budgets far exceed those of many industrialized countries. **Technological breakthroughs will most probably happen in these innovative companies, which usually have the brightest employees and latest technologies.**

For example, GAF A is an acronym for Google, Apple, Facebook, and Amazon, which are the four most powerful American technology giants. The market value of these four companies was estimated at USD 2,398 billion in 2017. For this set of private, non-state actors such financial power and market influence would be enough to impress in itself. There are many other giant technology companies too. **The way private sector companies collect and analyse data, create algorithms that are more sophisticated, develop disruptive technology and build their own global undersea internet cable systems, for example, already reflects their power and influence in**

There has been a lot of discussion lately about misinformation, which has been rife in social media. Private companies own the social media platforms, which people are using ever more frequently. As social media has become more effective, demands to limit the prevalence and potential disruptiveness of online misinformation have intensified. Currently, amid increasing pressure from governments and users, technology companies have also been taking steps to reduce the financial incentives for the creators of fake news and to enhance the transparency of material on their platforms. This is a good example of how shared responsibility is being created in the technological environment and preserving the strengths of democracy – one step at a time.

As technological advancements are becoming more influential and the role of private companies is increasing in both world politics and security, **a culture of shared responsibility will enhance the strength of democratic states and will be a powerful tool for countering hybrid threats.**

**There are three key starting points for creating this culture of shared responsibility. Firstly, the technology companies should be invited to the “tables” where governments are discussing and making decisions on security.**



**Engaging the private sector is an important step. Secondly, private sector companies must know their responsibilities and demonstrate their social responsibility** through

practical actions. **Thirdly, increasing transparency** – both in politics and in technology – is the foundation of trust, not least when it comes to security.

---

## Author

**Jarno Limnéll** is Professor of Cybersecurity at Aalto University, Finland, and an adjunct professor in three other Finnish universities. He also works for a private company. He has been working with security issues for over 20 years, and has a profound understanding of the global threat landscape, combined with the courage to address the most complex issues. Professor Limnéll has published a comprehensive list of works on security issues. His most recent book is entitled *Are you scared? Young people and the future of security*.

---

## Literature:

Carr, Madeline (2016) Public-private partnerships in national cyber-security strategies, *International Affairs* 92:1, 43–62.

European Commission (2016) Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats.

[http://europa.eu/rapid/press-release\\_IP-16-2321\\_en.htm](http://europa.eu/rapid/press-release_IP-16-2321_en.htm)

Internet Society (2017) Paths to Our Digital Future.

<https://future.internetsociety.org/wp-content/uploads/2017/09/2017-Internet-Society-Global-Internet-Report-Paths-to-Our-Digital-Future.pdf>

Morgan, Jonathon (2017) Facebook and Google need to own their role in spreading misinformation – and fix it, CNN.

<https://edition.cnn.com/2017/10/09/opinions/social-media-platforms-spreading-disinformation-opinion-morgan/index.html>

Munich Security Conference (2018) Munich Security Report 2018.

<https://www.securityconference.de/en/discussion/munich-security-report/munich-security-report-2018/>

Prime Minister’s Office Publications (2017) Government Report on the Future, Part 1.

[http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80120/13c\\_17\\_tulevaisuusselonteko\\_osa1\\_EN.pdf](http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80120/13c_17_tulevaisuusselonteko_osa1_EN.pdf)

Rosemont, Hugo (2016) Public-Private Security Cooperation From Cyber to Financial Crime, RUSI.

[https://rusi.org/sites/default/files/op\\_201608\\_rosemont\\_public-private\\_security\\_cooperation1.pdf](https://rusi.org/sites/default/files/op_201608_rosemont_public-private_security_cooperation1.pdf)

Statista (2018) Google, Apple, Facebook, and Amazon (GAFA) - Statistics & Facts.

<https://www.statista.com/topics/4213/google-apple-facebook-and-amazon-gafa/>

Warner, Sullivan (2017) Putting Partnerships to work, strategic alliances for development between government, the private sector and civil society, Routledge, New York.

World Economic Forum (2018) The Global Risks Report 2018.

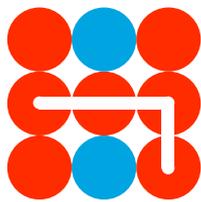
<https://www.weforum.org/reports/the-global-risks-report-2018>

The European Centre of Excellence for Countering Hybrid Threats  
tel. +358 400 253800 [www.hybridcoe.fi](http://www.hybridcoe.fi)

ISBN 978-952-7282-05-2

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) serves as a hub of expertise to enhance civil-military capabilities, resilience, and preparedness to counter hybrid threats with a special focus on European security and on EU–NATO cooperation.

The responsibility for the views expressed ultimately rests with the authors.



Hybrid CoE