Conference Report

Cyber-Security - Perspectives

By Arnold Koka

Euro Gulf Information Centre | info@egic.info | www.egic.info | ©2019

As the pervasiveness of the cyber-sphere grows in public life, so do the challenges that this domain poses to national and international actors. The growing weight that the cyber-sphere has taken in security, political and economic agendas around the world and calls for an expansion of awareness by policy-makers and relevant stakeholders on the need to improve interactions with the cyber realm.

Against this backdrop, on 14 May 2019, the Euro-Gulf Information Centre (EGIC) organised a high-level roundtable composed of cyber-security experts, namely: Arije Antinori (Stratcom Expert Geopolitics and OSINT Analyst); Sarah Backhman (PhD at Stockholm University and Consultant in Strategic Cybersecurity at Secana); Alexi Drew (Research Associate at the Centre for Science and Security Studies at King's College London); Andrea Gilli (Senior Researcher at the NATO Defense College); Corrado Giustozzi (Cybersecurity Expert at Agenzia per l'Italia Digitale, Journalist and Professor); Giulio Terzi di Sant'Agata (Former Ministry of Foreign Affairs, Former Ambassador, President CSE Cybsec SpA).

Major international events have shown that the virtual arena to be a pivotal platform – in some cases, battlefield – of economic, political and security interests in various dimensions.

In 2015, sophisticated cyber-attacks hit Ukraine's power grid systems, leaving hundreds of thousands without electric power around the country. The attacks – by some believed to have been led by Russian hackers – were repeated in June 2017 on a wider scale. Initially targeting Ukraine's government and businesses, a ransomware spread internationally, hitting network systems of institutions and companies through Europe, the United States and even Australia.

More recently, in May 2019, the Donald Trump administration declared a National Emergency, prohibiting executive companies from using foreign technologies believed to augment risks of sabotage by foreign players. The decision came after a cybersecurity crackdown by the US Government against alleged Chinese plans to infiltrate US IT networks through the production and the installing of the 5G technology by the Chinese-based Huawei.

This increasing internationalisation of cyber-risks must be a wake-up call for the international community. The threats posed to the digital domain cannot be overlooked, and an unprecedented level of cooperation between national and international institutions is required to contain them.

For instance, cooperation needs strengthening at the EU level, since its cyber-security apparatus still lacks a harmonised and unitary approach, as Corrado Giustozzi highlighted. One concrete necessity of further EU cooperation is to contrast cyber disruption of Critical National Infrastructures (CNI) – physical assets essential to the stable functioning of a society -a major threat to economic interests and to regional security. As Sarah Backhman underlined, 'Greater trust and synergy among states is needed. At the EU level the focus is still on pre-emptive measures when it comes to CNI, but responsive mechanisms are largely overlooked.' At this current historical juncture, when CNI have become appealing targets for hostile cyber-actors, the absence of a communal strategy becomes a hazardous risk.

The EU Commission is attempting to pull together a more comprehensive approach. The European Union Agency for Network and Information Security (ENISA) works in the direction of improving communication and sharing of information among EU members, an approach strongly welcomed by Corrado Giustozzi, also a member of the Permanent Stakeholder Group of the agency, who said "Forecasting dangers and future challenges can only take place by warning sharing. In that, ENISA is extremely useful".

A EU-wide approach is necessary, however, not only to face activities of hostile foreign powers who target physical and digital infrastructures but also to pressure large multinational companies to adopt effective security and privacy policies that, as in the case of Facebook and Twitter, have been overlooked for a long time. Major companies' economic and strategic relevance makes their impact comparable to that of state actors, as pointed out Giulio Terzi di Sant'Agata.

In addition, is worth pointing out the challenges posed by non-state actors, such as

terrorist groups and organised crime, who increasingly make a far and wide use of the cyberspace. Daesh's experience teaches vastly on their use for propaganda, recruiting and on-the-ground operations. Framing effective countermeasures against evolving actors and situations needs institutions able to pick up the pace not only in terms of technologies, but also of strategic perspectives, as argued Arije Antinori. In such context, on the 17th of May 2019, the EU Council established a framework which allows the EU to impose sanctions on entities responsible for cyber-attacks or attempted ones and even on those who provided financial, technical or material support. This undoubtedly constitutes a step forward. However, such framework still neglects mechanisms through which legal responsibilities for the attacks should be ascribed and the significance of the attack should be measured. NATO itself still lacks an official understanding about the kind of cyber-attack that would be a trigger for Article 5, meaning an attack on all the organisations' members.

Arguably, cyberattacks carry the most devastating potential when directed at political and economic targets. The ever-increasing relevance of ICT in politics has shed the light on the risks of their sabotage and misuse, including through Russia's alleged interference in US 2016 elections. Indeed, as underlined by Dr. Drew, the use of cyber technologies as instruments of international relations differs from one actor to another.

While Western democracies have initially failed to interpret social media as strategic tools, other actors have quickly understood their instrumental role in domestic and foreign politics. In this sense, Russia has worked to immunise itself against information risks through the usage of social media platforms. Russia-founded platforms as Telegram and VKontakte substitute in the country Whatsapp and Facebook: that shields Russian users from the same kind of information warfare put into action by Moscow on Western platforms, as in the case of the 2016 US elections.

Even apparently safe technological tools can be used for political or espionage purposes, stated Alexi Drew. A case among others is the adoption of the 5G network

technology. The 5G has raised concerns - as Terzi di Sant'Agata emphasised - regarding its possible hostile misuse and the fact that it could constitute a cyber-threat intentionally developed by China.

Due to its ubiquity, the cyber-sphere is often used with diverging security and strategic purposes. This makes education and specific technological awareness essential to both users and policy-makers.

To effectively deal with the cyberspace and its challenges and raise awareness about its complexities sharing of knowledge and wide-ranging expertise is pivotal to craft a needed global unitary approach. Such process has indeed been difficult in the past but today is needed more than ever.

EGIC through its conferences, analyses and events works constantly at building a network of experts with the aim to aid the work of policy-makers and improve discussion around security and awareness of the cyber domain.