Building Infrastructures: Reviewing Cypriot Cybersecurity Practices

Petros Petrikkos

Originally published with Global Risk Insights

https://globalriskinsights.com/2019/04/building-infrastructures-reviewing-cypriot-cybersecurity-practices/

A lack of attention in addressing Cyprus' cyberspace and security systems is a major problem for the country. The rise of newer technologies and threats require an upgrade in the existing systems. Regional developments also endanger obsolete technologies. This is an updated overview, detailing how Cyprus needs to address these issues within its administrative domains.

Introducing critical information security infrastructures

One of the biggest threats countries face today is data theft and misuse. The most vulnerable areas include telecommunications, public archives and records, and any other day-to-day societal functions. If vulnerable, attacks against these critical infrastructures could bring down an entire economy. The European Union has legal structures in place that authorise member-states to take decisive measures against matters of national security.

The introduction of the 2006 European Programme for Critical Infrastructure Protection led to a stronger focus on correcting critical infrastructure flaws. Additionally, within the EU Cybersecurity Strategy, the EU Network and Information Security (NIS) Directive monitors and supervises cybersecurity legislation. This falls under the authority of the European Union Agency for Network and Information Security (ENISA).

During the 2012 Cyprus-EU Presidency, a top priority was ENISA itself:

[blockquote style="1"]The Presidency places great emphasis on network and information security and will continue the work on the European Network and Information Security Agency (ENISA) and initiate discussions on the European Internet Security Strategy.[/blockquote]

With the introduction of the NIS Directive and the General Data Protection Regulation (GDPR), it was assumed Cyprus would immediately comply with cybersecurity legislation. Contrary to the NIS Directive, GDPR is a regulation. It is automatically binding on all member-states. This has allowed the Cypriot Commissioner for the Protection of Personal Data to impose fines and sentence those not complying.

Moreover, greater participation in research conferences was an important stepping stone. For instance, Cyprus hosted the 9th International Conference on Critical Information Infrastructures Security (CRITIS) in 2014. Nonetheless, as of 2017, key areas within the Cypriot economy remain exposed due to the lack of proper cybersecurity mitigation. For example, the state has no central authority for logging cybersecurity incidents. This means that the public sector has deficits that must be addressed and brought up to date with other EU member-states.

Private companies use

It seems that the private sector itself is much more receptive to ENISA frameworks rather than member-states' national bodies. Characteristically, private companies understand the need to mitigate cyber threats. The majority of companies within the Cypriot economy rely on strong cybersecurity mechanisms. This is because most companies provide a service-based product. Constant security updates and checks, as a result, would mitigate any potential risks in the private sector.

The current legal structure, however, makes it difficult to substantially mitigate or counter cybersecurity threats at the national level. Legal frameworks do little to stop cyber criminals from launching an onslaught. Up until recently, this was due to member-states like Cyprus lacking legal obligation. Consequently, private companies began assisting with cybersecurity practices by providing digital defence tools to both public and private authorities.

Despite the updates in tackling cyber crime and personal data violations, Cyprus still ranks poorly on antimalware defences on a global scale. Malware, DDoS, and ransomware attacks in Cyprus have typically targeted the financial and legal sectors. These are the most important economic sectors of the Cypriot economy. If these sectors are compromised, a serious chain reaction would have a huge impact on society. With the remnants of the 2012-2013 financial crisis still being felt, companies would want to avoid another attack at all costs.

Current deficits in Cypriot policy

Cyprus is a small state that needs to strengthen national and financial security.. During and after the Cyprus-EU Presidency, the state set out and completed its national cyber security strategy objectives within ENISA. These included core issues such as addressing cyber crime, protecting critical information infrastructures, and boost international cooperation and public-private engagement. Similarly, Commonwealth countries vowed in April 2018 in London to address cybersecurity issues as matters of international security. Cybersecurity, then, has become a top priority for Cypriot policy makers in recent years.

However, less emphasis was placed on mitigating cyber threats. As an EU member-state, Cyprus has transposed the NIS Directive and has taken the path towards full implementation of ENISA-related mechanisms. Even so, the state has yet to release a national strategy on network and information systems security. Additionally, the University of Oxford’s Global Cyber Security Capacity Centre (GCSCC) published a report on Cyprus in late 2017. The report assessed the maturity and basic cybersecurity capacities of the Republic of Cyprus. It highlighted that key security protection mechanisms such as a Disaster Recovery Plan (DRP) had not been fully developed.

Independent contractors, such as DataBack and NetShop have provided disaster recovery schemes to operators. These include nationalised agencies such as the Telecoms and the Electricity Authorities. With the exception of the recovery services broadly defined by the Computer Security Incident Response Team (CSIRT), however, no state-led authority has been established to put forward centralised DRP initiatives.

International security risks and controls

In a digital era, electronic warfare is the first line of assault. Currently, the Republic of Cyprus has a single active CSIRT. On the other hand, neighbouring Turkey has 7 teams. These teams are a combination of private and state-owned initiatives. Not only does this give Turkey a tactical advantage, it also poses a great security threat to Cypriot information security. With half of the island *de facto* divided and faced with a regional energy dispute, the intelligence implications are serious. Combined with the presence of Turkish troops in the northern part of the island, Cypriot security infrastructure is vulnerable.

In addition, the current outdated Cypriot intelligence apparatus leaves it vulnerable to terrorism and extremism. The Syrian conflict is happening only a few kilometres away from Cypriot coast. The presence of transnational syndicate networks such as that of Hezbollah in the Eastern Mediterranean also brings additional risks. Cypriot intelligence has had to rely on EU institutions in order to address screening concerns on migration. Due to the lack of reliable technology, Cyprus has turned to entities such as Europol for assistance.

Cyprus has, however, managed to meet some expectations on defence and security EU protocols. The Permanent Structured Cooperation (PeSCo) under the Common Security and Defence Policy (CSDP) is important for further EU-Cyprus defence integration. It also equips the state with some up-to-date security and intelligence policies. For instance, based on state perspective, Cyprus has identified important links between maritime and cybersecurity-related concerns. Ensuring proper checks on electronic systems enable the country to continue its energy programme.

On the information-gathering front, Cyprus has pursued the creation of an EU intelligence school together with Greece, within the PeSCo framework. This should help address its underdeveloped intelligence apparatus in the medium run, yet the effects of such a revolutionary step remain to be seen.

Moving forward: Useful recommendations

Cyprus must continue pushing for the mitigation of serious cybersecurity challenges, personal data leak, as well as information security breaches. The first step is raising sufficient awareness and mobilising the public. This is probably the best initial practice that may minimise the impact of attacks on policy, the economy, and defence. The rationale is rather simple: the correct application of existing knowledge is a powerful protection tool. Secondly, effective training in both the private and public spheres is a must. Knowledge alone is not sufficient in tackling cybersecurity risks. Thirdly, fulfilling more requirements within the CSDP framework would help the country optimise within an EU-wide framework.

Finally, Cyprus should both centralise and expand on its cybersecurity practices. On the one hand, it needs to log any nationwide incidents for early warning and protection. On the other hand, it needs to incorporate more than just one CSIRT. Small states like Cyprus have a natural advantage: they can easily direct their bureaucracy towards boosting their cyberspace. This may involve anything from protection to even intelligence and reconnaissance. Unfortunately, Cyprus has yet to realise that it has the capacity to develop these tools, as a largely services-based provider in the Eastern Mediterranean.