Is Greece ready for the Digital Era?

Andrew N. Liaropoulos

(Assistant Professor, Department of International and European Studies, University of Piraeus, Greece)

Publication date: 18 July 2020

Over the past months, Greek governmental websites have been attacked and as a result, many of them went offline. Websites affected by the cyber-attacks included among others the Greek Parliament, the Ministry of Foreign Affairs, the Ministry of Finance, the National Intelligence Service, the Athens Stock Market and several Greek businesses. Media reports have attributed the attacks to Turkish hackers. After the attacks were revealed, a Greek hacker-group called Anonymous Greece, responded by launching cyber-attacks on Turkish websites. Such incidents are common and take place on a daily basis. Nevertheless, cyber-attacks consist only one part of the answer to our question.

Greece, as any other state, faces enormous challenges in cyberspace. Cyberspace has technical and structural uncertainties (e.g. complex governing structure, rapid development of Information Communication Technologies, non-territorial nature, diffusion of power) that project complexity and ambiguity for its users and mainly for the policy-makers. Cyberspace represents the backbone of our society. From the protection of critical information infrastructure, to the smooth functioning of the digital economy and the running of online platforms, states are called upon to provide security and become resilient. But how can we measure whether a state is prepared for the legal, political and security implications that cyberspace poses in our everyday life? How can we measure resources and assess effects?

Various indicators and metrics can be applied in order to assess the level of national cybersecurity. The International Telecommunication Union (ITU) has developed the Global Cybersecurity Index (GCI)[1] that measures the commitment of countries to cybersecurity at a global level. Since cybersecurity involves many industries and sectors, each country's level of development is assessed based on five sections: legal measures, technical measures, organizational measures, capacity building and finally cooperation. The rationale behind the GCI is to highlight the need for global synergies

[1] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

in the areas of cybersecurity. Therefore, this index reviews developments and initiatives regarding law enforcement, justice departments, educational institutions, ministries, private sector actors, public private partnerships, inter-agency partnerships and bilateral agreements. In 2018, Greece was ranked 77th at the Global Cybersecurity Index, due to the absence of a strong and efficient legal and regulatory framework. Nevertheless, over the past two years Greece has taken all necessary steps to secure its cyberspace. In 2018, Greece issued both the National Cyber Security Strategy and the National Law on security of network and information systems.[2] As a result, in the coming 2020 report, Greece is expected to get a higher score, based on the reforms that have taken place.

Another index, which measures the quality of ICT networks, internet activity and skills, e-government, ICT in schools and the level of broadband connectivity, is the Digital Economy and Society Index (DESI), developed by the European Commission.[3] In the DESI 2020, Greece was ranked 27th and scored 37.3. Greece belongs to the low cluster of the EU member states and needs to boost innovative businesses and develop digitization plans for the industry.

In May 2020, the National Cyber Security Index (NCSI) published its report, which includes cybersecurity data on 160 countries.[4] The NCSI measures countries' level of cybersecurity and provides an overview of their readiness to prevent and fight cyber-attacks. Surprisingly enough, Greece has been rated as the most prepared country to face cyber-attacks, followed by the Czech Republic and Estonia. Greece has scored an impressive 96.10 at the National Cyber Security Index, which measures the cyber security capacities that are implemented by the government. Greece has sorted out the legal and regulatory framework that involves national cybersecurity units, like CERTs, the cyber command and the digital forensics unit. Inadequate laws and policies will only produce chaos, when a state has to react to a large-scale cyber-attack. Responding successfully to the full range of cybersecurity challenges that a state faces, is not only a matter of capabilities, but also one of responsibilities, of identifying who has the jurisdictional authority to respond. Greece seems to have done its homework regarding the publication of cybersecurity policies and the establishment of the necessary units, but then again, this is only part of the story.

The purpose of this short note is not to provide a negative or positive answer to the question raised, but rather to highlight the fact that Greece still has a long way to go, in terms of adjusting to the needs of the digital era. Strengthening academic programmes in the field of cybersecurity and collaborating with professional certification bodies, are areas that will enable Greece to transform the national labour market to meet the demands of tomorrow. For example in many countries, universities tend to have partnerships with state security institutions. The benefit of such a partnership is to support knowledge transfer and accelerate the integration of students into the needs of their potential employers, be that the public sector, or even the private sector that provides services to the government. Likewise, cooperating with professional

[2] George Drivas, Leandros Maglaras, Helge Janicke and Sotiris Ioannidis, 'Assessing cyber security threats and risks in the public sector of Greece', *Journal of Information Warfare*, 19, 1 (2020).

[3] https://ec.europa.eu/digital-single-market/en/scoreboard/greece

[4] https://e-estonia.com/the-national-cyber-security-index-ranks-160-countries-cyber-security-status/

certification institutions, will offer a soft standardisation of the minimum knowledge and requirements for the public and the private sector, enabling rapid labour market qualification.

Concisely, Greece needs to crystallize its national vision for the digital era. The clearer the vision, the easier it will be for all the key stakeholders to ensure a more comprehensive and consistent approach.