Center for Cyber Security and International Relations Studies

THE

Cyber Short Analysis

- July 2018 –

The importance of education for cyber security

‘ A minimum part of risk factors derives from technological tools, […] the others are caused by human and cultural dynamics […]’

Luigi Martino

Luigi Martino, Director of CSSIRS

Luigi Martino

Head of the CSSIRS, a specialized observatory of the CSSII at the Department of Political Science (University of Florence).Currently, Luigi is Ph.D. Candidate in Human Rights and Global Politics, School of Advanced Studies Sant’Anna, Pisa with a Research Project on “Improving Cybersecurity for Critical Infrastructure: The Public-Private Partnership Model Against Cyber Attacks”.

Opinion of the expert

Dear friends and colleagues,

I am extremely proud to present our new short analysis, a series of brief opinions written by national and international experts and scholars in the field of cyber, aimed at collecting different perspectives and approaches to this very wide subject. We chose a first topic related to education to highlight our approach to cyber security, based on promoting knowledge and awareness, which consequently is a main objective for this project.

The relevance of education and academic training in the cyber field is strictly interconnected with the types of threats to which everyone is exposed in the cyberspace. In this complex arena, a minimum part of risk factors derives from technological tools, as software, hardware etc, while the majority is caused by human and cultural dynamics and by the lack of knowledge and consciousness of the risks themselves. This is true for all the sectors of society, since cyber security is becoming a main component of our daily life as a whole. Consequently, the human-related risks have to be taken into consideration especially by policy decision makers and managers, since their behaviour and choices have a strong impact on national safety and security.

Since cyber security is a multidisciplinary subject, training and education should not solely focus on technological aspects, but should also encompass legislative and institutional perspectives. One of the principal challenges in this field concerns the competence of public and private decision makers, who often lack specific skills and knowledge that are of a paramount importance to reach the expected results. The Center was created to study the issues related to the cyber world adopting a multidisciplinary approach with a particular attention to the legal, ethical, economic and policy aspects of cyberspace.

Therefore, the monthly appointment of our short analysis wants to become an occasion to explore and analyse many aspects and perspectives concerning this broad domain. We also encourage our younger associates and collaborators to provide their researched opinions in the second session of the document. We would also invite you, the readers, not to hesitate to contact us providing ideas for the next topics, giving opinions or asking specific questions: we want this project to become as interactive and dynamic as possible, by promoting an effective diffusion of the "cyber security" culture through a genuine, educative and stimulating dialogue with our readers.

Opinion from the Center

Daniela Giordano

Graduated in Political Science at LUISS University in Rome. Currently enrolled in the joint Master program in International Security Studies at Sant'Anna School for Advanced Study and University of Trento with a final thesis on cyber security on critical infrastructures.

Focus: Cyber Hygiene (Sociology)

The online safety and security of an individual, a company or even a state depends only partially from the technical instruments employed. A vast majority of cyber attacks could have been avoided or at least have less impact if cyber hygiene standards and rules would have been taken more seriously into consideration. ENISA defines cyber hygiene as 'the equivalent of establishing simple routine measures to minimise the risks from cyber threats'. Since cyber security is often depicted as a chain, the weakness of a single ring can endanger the rest of it. Therefore, the education and training to cyber security should not be limited to top level managers or decision-makers, as they are just one of the social layers, but encompass a 'cultural revolution' in the way we think our own security. In order to achieve it, we need to acknowledge the level of diffusion of the cyberspace and especially its influence and importance in our everyday life. So in conclusion, on one hand the training in this sector should not be concentrated entirely on those who are considered the final decision-makers, but spread best practices and standards also (and in some cases, especially) to the lowest levels of a company or a society. On the other hand, education should start from the very primary school so to create a new generation which would be able to embrace both the risks and the opportunities of this 'fourth industrial revolution' better than their predecessors.