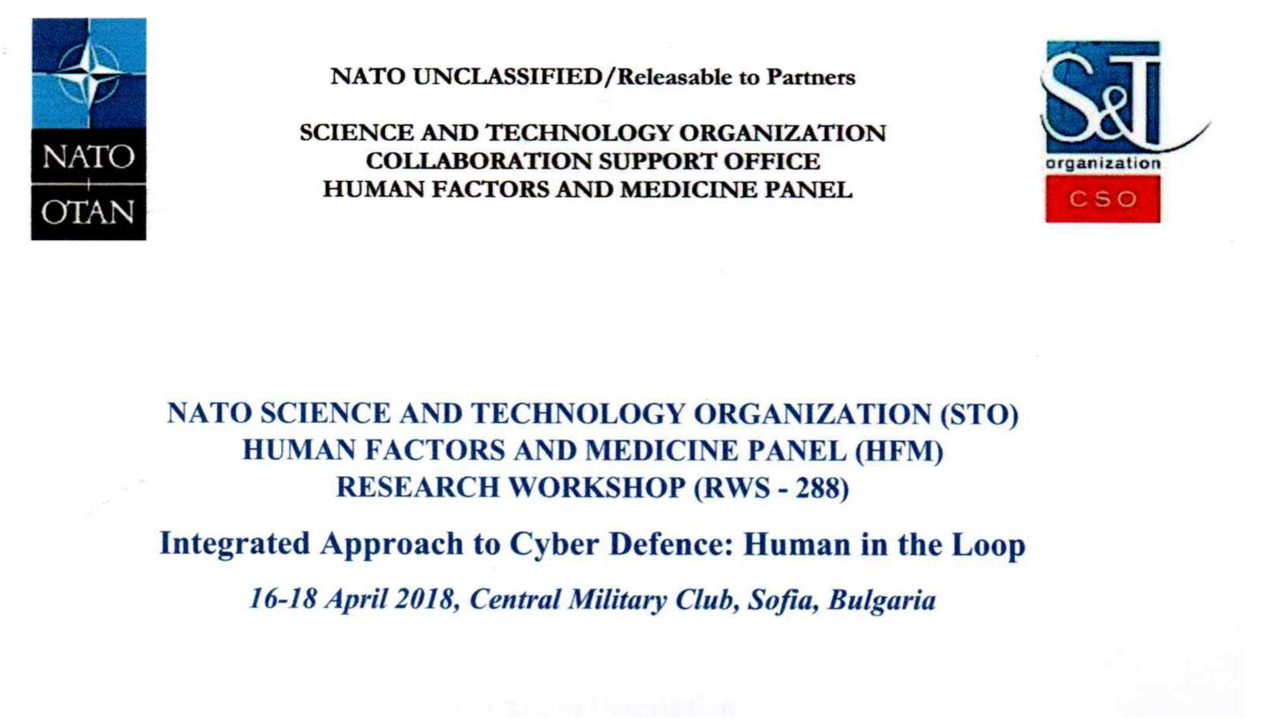

NATO UNCLASSIFIED/Releasable to Partners

SCIENCE AND TECHNOLOGY ORGANIZATION
COLLABORATION SUPPORT OFFICE
HUMAN FACTORS AND MEDICINE PANEL

NATO SCIENCE AND TECHNOLOGY ORGANIZATION (STO)
HUMAN FACTORS AND MEDICINE PANEL (HFM)
RESEARCH WORKSHOP (RWS - 288)

Integrated Approach to Cyber Defence: Human in the Loop

16-18 April 2018, Central Military Club, Sofia, Bulgaria

CYBER DEFENCE: CENTRALITY OF THE HUMAN FACTOR, MAIN DEFENCE AND PREVENTION TOOLS

report held by

Brig.Gen.(ret) Antonio Trogu

Senior expert of EIRC Foundation, Master's degree in Strategic Sciences, Certificate of the Institute for Italian Advanced Defense Studies.

Summary

Cyber threats are becoming more and more serious, commensurately whit the digital dependency of more thecnologically advanced countries. Cyber space is a cross cutting domain encompassing the traditional land, sea, air and domains with a lack of geo specifity and limited scope for attribution. The cyber security mission will require a workforce that possesses the necessary skills to lead cyber security missions and solutions, while ensuring the future security of the national critical infrastructure. The Human factors in cyber security are perhaps the biggest challenge when building an effective threat prevention strategy. A general overview of the countermeasures adopted by the Italian defense: Joint Cyber Command

Cyber space (cyberspace) is the term conventionally used to refer to the environment within which the operations occur they use the internet. the reduction of the costs of access to the network and the development of the broadband will result in further growth of cyberspace, making it an increasingly crucial factor for economic and social growth.

Cyber threats are becoming more and more serious, commensurately whit the digital dependency of more technologically advanced countries. cyber space is a cross cutting domain encompassing the traditional land, sea, air and domains with a lack of geo specifity and limited scope for attribution, there is a progressive increase, quantitative and qualitative of attacks and criminal threats with the most disparate purposes, in that "land of medium "which has now become cyberspace: from fraud and computerized extortion the theft of identity and sensitive data, up to and including espionage sabotage, including purely emulative vandalism. Attacks that can also not be targeted to hit a specific subject, selected in base to certain characteristics, but to randomly damage a number indefinite of subjects sensitive to the threat predisposed by the criminal.

Cyber attacks are becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and euro-atlantic prosperity, security and stability. foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks. NATO strategic concept (lisbon summit 2010).

Disputes become armed conflicts when politics fails and now cyberwar or information warfare is the digital continuation of, and sometimes the replacement for, conflict. cyberwar tends to erase the threshold between reality and simulation, between life and play and between conventional conflicts, insurgencies and terrorist actions.

That of cyber-security is "one of the most challenging challenges of this time and will mark the future of the international community".

Cyber security, also known as computer security or IT security, is the protection of computer systems from the theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide it includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures the first one is a specific organization, which comprises personnel, logistics, doctrine, operations simplifying, in general, the mission is the defense of one's own information and assets and guarantee and optimize the solidity of its infrastructures and to enhance the cyber defense capability through:

- research and development;
- lessons learned;
- awareness and training.

The cyber security mission will require a workforce that possesses the necessary skills to lead cyber security missions and solutions, while ensuring the future security of the national critical infrastructure. It is necessary to delineate criminal scenarios of risk, also in order to indicate to national governments and to the services of intelligence where to allocate efforts and resources not only for law enforcement purposes but above all for prevention purposes. these scenarios can be decomposed in the following elements:

1) **WHO**, ie actors, structures and emerging organizational models of the crime;
   "virtual market that offers highly specialized products and services to perpetrate criminal activities and / or cyber threats, limited actions / projects, limited in time and aimed at objectives specific, using cyber-freelance professional criminals who, led by the profit, sell skills and tools (malware, zero-day exploits, or access botnet) to criminal and terrorist groups".
2) **WHAT,** or risks in terms of targets and victims;
   "in cyberspace, threats challenge the stability, prosperity and security of all our nations, and cyber-attacks can be launched by states, terror groups, criminal organisations or individuals who aim at destroying or damaging information systems and data.
3) **HOW**, that is the modus operandi;
   general cybercrime trends indicate more sophisticated and multi-purpose attacks,an increase in the number and type of attack, as well as the number objectives and victims and consequent economic damage. The progressive specialization of cyber criminals corresponds specular to the creation of a network of diversified and personalized services for activities criminals.

Several very diverse actors play important roles in the formulation of cyber policies, while most of them are governmental actors, private actors — such as industry — play key roles too. At national level, for instance, the ministries of defense, the interior and justice, law enforcement agencies and intelligence agencies, and also universities, including research centres specialized in defense and warfare studies, normally play a role. Cyber threats represent a serious danger for national security and for the economic stability of our countries. this requires each of us - businesses and individuals, and not only institutions - to behave responsibly. the most frequent vulnerabilities, in fact, are more attributable to people than to technology, the privatization of responses, however, must be regulated to avoid possible abuse.

It is therefore necessary to consider the approach to the ethical aspect of the problem: ethics, moral principles that govern a person’s behavior, is a critical part of any sound cyber security defense strategy. without clear ethical standards and rules, cyber security professionals are almost indistinguishable from the black-hat criminals against whom they seek to protect system and data.

"Education and awareness", are activities to support the creation of so-called cultural and situational awareness, fundamental in all strategic environments, from peace support operations (psos) to social and economic conflicts.

But it is equally important the creation of institutional synergies in an integrated, even supranational, system able to deal effectively with the complex and multi-faceted challenges of the cyber threat.

A similar scenario has contributed to the proliferation of several centers of study on cyber security, many of which have acquired, possibly ex post, the label of "center of excellence" fundamental for an effective contrast of a threat cyber in continuous evolution:

- ✓ ACQUISITION AND UPDATING OF TECHNOLOGICAL SYSTEMS;
- ✓ CONTINUOUS EDUCATION OF ALL PERSONNEL;
- ✓ TRAINING AND PERIODIC TRAINING OF THETECHNICAL STAFF;
- ✓ INTERNATIONAL COOPERATION AND CONTINUOUS EXCHANGE OFINFORMATION ON IT SECURITY.

The human factors of cyber security represent the actions or events when human error results in a successful hack or data breach. Most attacks per computer systems are carried out thanks to a human factor component (factor h), the human component it can be both of a conscious nature and of an unconscious nature, but in both in cases it is often decisive to complete an attack successfully.

The centrality of the human factor, the growth and dissemination of skills means need to identify professionals able to plan and design activities' intervention in response to cyber attacks and identifying the training and professional development required. one key lesson is that while technical upgrades are important, minimizing human error is even more crucial.

The goal is how we should recruit, educate, train and develop cyber operators. cyber security provides a great opportunity for national industry and for universities, which are called upon to take charge of cyber operators’ advanced training. this should desirably begin with it-specialized high school education defense will have to recruit civilian operators through specific competitions, while still relying on its own resources. available technologies being equal, the human factor will always make the difference.

Unlike most of computer crime/misuse areas which are clear cut in terms of action and legalities, computer hacking is more difficult to define. computer hacking always involves some degree of infringement on the privacy of others or damage to computer-based property it is defined as the activity of illegally using a computer to access information stored on another computer system or to spread a computer virus: ***hacking*** is now much more sophisticated and harder to detect than a few years ago. So we can ask: who is a hacker? do we know his way of thinking ? he is human not a computer !

A recent nuix black report surveyed 70 of the world's best professional hackers and found that 88 percent of hackers can break into their desired system and get through cyber security defenses in 12 hours or less. it only takes an additional 12 hours for 81 percent of hackers to find and take valuable data. when cyber security professionals can better understand the mysterious nature of hackers and how they work, they may be able to better protect their own systems. cyber security involves "legal" hacking, to catch a hacker, one has to think like a hacker.

"IF YOU KNOW THE ENEMY AND YOURSELF, YOUR VICTORY IS CERTAIN. IF YOU KNOW YOURSELF BUT NOT THE ENEMY, YOUR CHANCES OF WINNING AND LOSING ARE EQUAL. IF YOU KNOW NEITHER THE ENEMY NOR YOURSELF, YOU WILL SUCCUMB IN EVERY BATTLE"

SUN TZU THE ART OF WAR

The recent acknowledgement of the relevance of the cyber domain will lead many nations to set up military commands exclusively in charge of conducting cyber operations, nato and its allies rely on strong and resilient cyber defences to fulfil the alliance's core tasks of collective defence, crisis management and cooperative security. nato needs to be prepared to defend its networks and operations against the growing sophistication of the cyber threats and attacks it faces.

In Italy, in compliance with the defense white paper. defence has created a joint cyber command consistently with the objectives that have been defined within both the EU and NATO, which include the creation of robust cyber defense and infrastructure defense capabilities, the joint cyber command is already running and will be achieving full operational capability in 2019.

The fundamental task pertaining to the joint cyber command is protecting the military system from cyber threats, which thrive on the logic, technological, physical and social dimensions. these threats have an intrinsic feature: they are pervasive. in fact, they have no boundaries and almost never reveal the real identity and intent of the attacker. however, a distinction should be drawn between what constitutes an attack in criminal terms – namely an offence for stealing data, spying, attacking, disrupting - and what is a real military attack on the national system, and will need to be assessed as such in the future. at present, the command is strengthening its cyber security capabilities, the defense of its own networks, and the protection of operations especially in theatres of operations abroad. this is all done without neglecting national territory and focussing on the protection of command and control systems in order to ensure that operations are effectively conducted on the field, especially to guarantee the safety of deployed forces. cyber security provides a great opportunity for national industry and for universities, which are called upon to take charge of cyber operators advanced training. this should desirably begin with it-specialized high school education. defence will have to recruit civilian operators through specific competitions, while still relying on its own resources.is in progress the creation of a training organizationwithin the italian armed forces school of telecommunications in chiavari, where virtual firing ranges will be established with cyber operations training purposes. regarding the human factor, more than 70% of the overall capability of any cyber environment is supposed to depend on human skills. therefore, operators should be carefully selected and trained, also through the support of academia and research, as well as other organizations within the national industry.

“Available technologies being equal, the human factor will always make the difference”.

Develop and maintain expertise in all matters relating to cyber defence. maintain expertise to provide direction and guidance to the nato civil and military bodies on cyber defence capabilities, implementations and procedures. ensure collaboration with and updates to relevant nato bodies on issues such as intelligence, counter terrorism, communication and information systems (cis) and security committees and communities relevant to cyber defence.

"IN THE CHALLENGE OF ARTIFICIAL INTELLIGENCE, BETWEEN THE ALGORITHM AND THE MAN, IT IS FUNDAMENTAL TO ALWAYS KEEP THE MAN AT THE CENTER”.WE ALL MAKE MISTAKES. WE ARE ONLY HUMAN, AFTER ALL. UNFORTUNATELY, WHEN IT COMES TO CYBER SECURITY, THAT’S ALSO KIND OF THE PROBLEM. THE HUMAN FACTORS IN CYBER SECURITY ARE PERHAPS THE BIGGEST CHALLENGE WHEN BUILDING AN EFFECTIVE THREAT PREVENTION STRATEGY”.