Cyber defence: centrality of the human factor

main defense and prevention tool.

Brig, Gen, (ret) Italian Army
Antonio Trogu
18 aprile 2018

Cyber space (Cyberspace) is the term conventionally used to refer to the environment within which the operations occur they use the Internet.

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

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

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)

CYBER SECURITY, ALSO KNOWN AS COMPUTER SECURITY OR IT SECURITY INCLUDES:

- CONTROLLING PHYSICAL ACCESS TO THE HARDWARE
- PROTECTING AGAINST HARM
- MALPRACTICE BY OPERATORS, WHETHER INTENTIONAL, ACCIDENTAL

MISSION

DEFENSE OF ONE'S OWN INFORMATION AND ASSETS AND GUARANTEE AND OPTIMIZE THE SOLIDITY OF ITS INFRASTRUCTURES AND TO ENHANCE THE CYBER DEFENCE CAPABILITY THROUGH:

- RESEARCH AND DEVELOPMENT
- LESSONS LEARNED
- AWARENESS AND TRAINING

CYBER SECURITY MISSION

- ✓ WILL REQUIRE A WORKFORCE THAT POSSESSES THE NECESSARY SKILLS TO LEAD CYBERSECURITY 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

ELEMENTS OF THESE SCENARIOS

WHO – WHAT - HOW

- **WHO** : 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

ELEMENTS OF THESE SCENARIOS

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"

ELEMENTS OF THESE SCENARIOS

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 SPECULARLY TO THE CREATION OF A NETWORK OF DIVERSIFIED AND PERSONALIZED SERVICES FOR ACTIVITIES CRIMINALS

ACTORS INVOLVED

SEVERAL VERY DIVERSE ACTORS PLAY IMPORTANT ROLES IN THE FORMULATION OF CYBERPOLICIES ,WHILE MOST OF THEM ARE GOVERNMENTAL ACTORS, PRIVATE ACTORS — SUCH AS INDUSTRY — PLAY KEY ROLES TOO.

AT NATIONAL LEVEL, FOR INSTANCE, THE MINISTRIES OF DEFENCE, THE INTERIOR AND JUSTICE, LAW ENFORCEMENT AGENCIES AND INTELLIGENCE AGENCIES, AND ALSO UNIVERSITIES, INCLUDING RESEARCH CENTRES SPECIALISING IN DEFENCE 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 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, KEEPING IN MIND THE ETHICAL ASPECT.

ETHICS: MORAL PRINCIPLES THAT GOVERN A PERSON'S BEHAVIOR

WITHOUT CLEAR ETHICAL STANDARDS AND RULES, CYBERSECURITY 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

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.

THIS 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.”

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 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

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? IT 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.

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” (ETHICAL) HACKING

TO CATCH A HACKER, ONE HAS TO THINK LIKE A HACKER.

“ETHICAL HACKING” IS THE PRACTICE OF TESTING SOFTWARE OR SYSTEMS TO TRY TO EXPOSE SECURITY FLAWS. IS THE METHOD OF LOCATING WEAKNESS OR POTENTIAL THREATS IN THE SYSTEM AND IMPROVE THE SYSTEM SECURITY TO MINIMIZE THE ACT OF HACKING BY POTENTIAL HACKERS. IT IS ALSO KNOWN AS PENETRATION TESTING, INTRUSION TESTING OR RED TEAMING

SOFTWARE DEVELOPMENT COMPANIES HAVE EMPLOYED HACKERS FOR DECADES TO ENSURE THAT NOBODY CAN BREACH THEIR PRODUCTS.

"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)

ITALIAN JOINT CYBER COMMAND

IN COMPLIANCE WITH THE DEFENCE WHITE PAPER. DEFENCE HAS CREATED A JOINT CYBER COMMAND CONSISTENTLY WITH THE OBJECTIVES THAT HAVE BEEN DEFINED WITHIN BOTH THE EU AND NATO.

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 ARE PERVASIVE THEY HAVE NO BOUNDARIES AND ALMOST NEVER REVEAL THE REAL IDENTITY AND INTENT OF THE ATTACKER.

A DISTINCTION SHOULD BE DRAWN BETWEEN WHAT CONSTITUTES AN ATTACK IN CRIMINAL TERMS AND WHAT IS A REAL MILITARY ATTACK ON THE NATIONAL SYSTEM.

AT PRESENT, THE COMMAND IS STRENGTHENING ITS CYBER SECURITY CAPABILITIES, THE DEFENCE OF ITS OWN NETWORKS, AND THE PROTECTION OF OPERATIONS ESPECIALLY IN THEATRES OF OPERATIONS ABROAD.

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.

IS IN PROGRESS THE CREATION OF A TRAINING ORGANIZATION WITHIN 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.

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.

EXPERTISE DEVELOPMENT

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)

"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.