

Cyber Warfare

Introduction

Every country has its right to defend itself by all appropriate means. Defence industries arose to satisfy demand for armies and doesn't seem to stop growing. This industry is driven by daily progress in advanced defence or offence technologies that make all the previous advancements obsolete. There are very few countries whose wealth allows to keep up with this speed. Even the best economic countries can't afford to develop technologies too advanced due to high expenses required for such programmes.

Any conventional army needs to be well equipped and well organized. Equipment is not the only expense because organization of the army is much more important. Organization is distribution of correct information in exact scale and timing. Every army needs information and telecommunication network, every army is based on logistics and every army needs to know the enemy. Information age doesn't show only in business but also on the battlefield. The information distribution needs to be done much faster; enemy movement must be communicated more precisely; troops need to be deployed more exactly and decisions have to be based on more accurate information. This shows that armies rely more and more on information, but they don't realize that information is an asset with great value that needs to be protected. All the effort to protect the information was targeted on physical security (eg. Limiting access to the information), but today with internetworking and teleworking there are other risks that need to be taken into account. Weaknesses in logical security enable attackers do all what is possible with conventional weapons (destruction of infrastructure) as well as weapons of mass destruction (nuclear reactor meltdown)

Cyberwarfare

Cyberwarfare is a relatively new type of weaponry with various effects on the target. It doesn't have any limitations of use and can achieve most of the goals set.

Weapons

Cyber weapons are usually basic programs that have the objective to defend or attack a target. Most of them are freely available on the internet but some more sophisticated or newer ones are kept privately or are commercial.

Detection

Systems in this category have the goal to detect possible attackers and identify what are they trying to do and possible where they are.

Detection can be based on expert knowledge (if I hear bullets flying then somebody is attacking us) or based on standard behavior (if a patrol doesn't come back from recon mission on time there might be an attack imminent).

Tools in this category are

- Intrusion detection systems
- Security monitoring
- Log analysis
-

Prevention

Stopping the attacker is the primary concern even if the attack has not been identified (locking the entrance door is always a good idea). Most of the attacks are very simple and straightforward just like testing each door if it is open and a good prevention is to simply lock it, unless somebody expects an army trying to enter (but then other preventive measures apply).

Main tools in this category are:

- Firewalls
- Authentication systems
- Authorization systems

Target Identification

Network scanners

System scanners

Vulnerability scanners

Attack

Here come all the tools that use the vulnerability of the system or application and achieve the objective an attacker wants. There are too many tools here to mention them as for every vulnerability there is more than one tool available.

It is also important to mention internet worms, that are automated tools misusing certain vulnerabilities and self-replicating themselves from one system to the other.

Another group are Trojan horses that can be deployed on the system to gain access to

it later or to create a covert channel to obtain important information.

Deception tools

Deceiving the enemy is also important in case a distraction is needed to perform an attack or to slow the detection time of it. Here belong these subcategories:

- Log modifiers
- Distributed attack systems
- Root-kits
- Stealth tools

Strategy and Tactics

The acclaimed British strategic thinker B.H. Liddell-Hart approached strategy from two different perspectives. He differentiated between a grand strategy and military strategy. Liddell-Hart's grand strategy focused on a nation's ability to coordinate and direct all resources of a nation toward the attainment of a political objective. Military strategy was more narrow, related to the execution of a battle plan or the projection of military force.

In Cybersecurity there is no difference between military and civilian infrastructure as many targets are non-military but indirectly are involved in military infrastructure. Disrupting economy or damaging image of a public infrastructure can wield much larger effect as weapons of mass destruction and therefore it is necessary not to limit the tactics or a strategy with any boundaries in order to get a global understanding of what attackers can gain or lose.

Strategies are based on certain behavior that defines the acting party. In cyber-security there are 3 major types (if not counting chaotic behavior)

Reactive behavior

Here strategy is based on action that can be seen or reported in any way. It reacts upon it with the appropriate response by increasing the awareness on that weakness.

As an example US security started to concentrate on airport security after September 11th incident. Or increasing awareness on information security after extensive cyber-attacks from china and other not "pro-american" countries.

This behavior strengthens those points in defence where attacks already happened, which means that there will be always several successful penetrations at the beginning. Although it seems as in longterm infrastructure may reach a point where the systems would be secured sufficiently, but the fact is that with introduction of new software or new updates (and this happens very often) there are new security holes introduced which may be misused in time.

Infrastructures with limited security resources are very often using this behavior to manage security. This means that security team in charge is either not very experienced or there is not enough people devoted to maintain IT systems. Depending on the response on a system breach there might be conclusions drawn upon their cybersecurity strategy (especially incident handling and security monitoring). By analyzing the security vulnerabilities of their systems it is possible to see the history of attacks upon their infrastructure.

There is also another alternative to this behavior, which is learning from mistakes of others, but not always can solutions of others be used to increase security of a bit

different infrastructure.

Planned behavior

Importance of planning is already well known to project managers, but due to the nature of IT infrastructure it is not always applicable. IT infrastructure can't be kept strictly static and not change to fit the work needs of its owner. To keep up with the progress in IT field as well as match the requirements for functionality in a very short time it is not possible to keep everything planned and well documented.

It is similar in national security planning where detailed plans won't work as expected as they cover huge economic; military and other systems that are changing very often and are not well documented.

In a best case with appropriate security planning well thought of and implemented appropriately can achieve decent level of security defense.

In former communist countries planning was done in almost every part of the state, but although many scenarios were thought of one aspect wasn't so much covered and that was human resources. Due to unexpected deviations in human behavior the whole system collapsed.

Cyber-security can be very well planned but the plan can't cover all scenarios and by not employing capable and experienced security people who can adopt the response there would always be a risk of a break-in.

If companies lack skilled people to operate defensive security measures or keep the systems secured (this is very often the case) appropriate response would follow after a long period of investigation and escalation. By knowing the procedures used by external companies an attacker can predict specific behaviors that would follow and adjust the cyberattack to prevent any response.

A risk may be to underestimate the possibility of having outsourced managed security system that might be difficult to overcome. This trend gains importance in middle-sized or progressively thinking companies and if implemented nation-wide can be a very effective measure.

Proactive behavior

Previous behaviors were trying to cover known risks and vulnerabilities, but what if there is something new that wasn't reported or documented? In such case this attacks would remain undetected and would be identified as anomalies. For detecting and preventing also unknown new attacks it is necessary to be highly flexible and "be the first to know" your weakness.

A security strategy that concentrates on identifying its own potential weaknesses and covering its own holes is based on proactive behavior.

There are many functions that fall under proactive behavior category:

- ⊗source code review
- ⊗formal functionality proving
- ⊗traffic analysis
- ⊗self penetration testing
- ⊗self-adaptable security measures

There are already some security solutions and products on the market but are not very capable due to lack of skilled people to operate it. Formal functionality testing and source code review is not done in necessary scope to insure the safety of such system.

Several countries already started investigating this field and started adapting some parts of their systems. China already invested a lot into building large and well trained cyber-security force or USA has built national cyber-security research centers to concentrate security experts and skilled engineers to improve bits and pieces of national cyber-security.

Proactive behavior needs highly skilled people and very tight security system in place and therefore it is important to keep highly skilled people in the country to either ensure its own security or to develop security systems that do it.

National security strategy

This is more an utopistic approach as it is not possible to integrate and synchronise all the parts of one nation into one cyber-defense initiative, but it should be the goal of any cyber-security initiative.

The main goal here is to secure the nation from the network provider side up to the end-user. There is one general security standard and security policy which is being implemented and audited by authorized experts. Central electronic warfare center is responsible of handling incidents that are reported by any entity in the country.

Educational system is capable of providing sufficient number of security experts and research capabilities to ensure implementation of national security strategy in every important infrastructure .

Attacking such system is extremely hard and may be only done from inside near by the target in order to minimize the possibility of detection or prevention. Such attacks require cooperation with conventional special forces that help the cyber-attack team to get to the target as close as possible and gain access to its data or functionality.

People

Security is based on 3 aspects: people; systems and procedures. As systems and procedures are developed by people, human resources are the key to cyber-security defense initiative.

Experts

The core of a cyber-security defense force are the people with security knowledge. These are not administrators who are able to install a firewall, but these are people who design and develop firewalls and other security measures.

Without these people a country or a company needs to rely upon external help that may or may not be successful.

Position of a security expert is similar to a nuclear scientist, who can invent and develop deadly weapon for any state that is willing to pay for his research.

Intelligence

Information about the enemy is according to Sun Tzu the key to success in the battle or warfare. Gathering information about enemy tools and cyber-security systems is as valuable as knowing what kind of weapons and soldiers enemy has. Even on a company level it is important to know what kind of new security tools are on the market and what kind of security problems were discovered recently. Also information about security experts may be valuable in case of recruiting needs.

Hackers

Defense force is one side of cyber-security but it is also necessary to have offense capabilities. For the training scenarios as well as for identification of existing and new security holes in systems hackers are important.

Very often ex-hackers tend to do security consulting but the major difference between a hacker and security expert is that a hacker needs to identify one hole while the security expert has to cover them all.

System programmers

With all the knowledge of security requirements and new security holes, there needs to be somebody who integrates and modifies the software/hardware or a solution. Knowledge of a system and skills in programming are necessary for progress of the IT industry as well as cyber-security.

Defense

Information systems have many potential weaknesses, but whatever they are if they don't operate there is a problem.

It is the scale of this problem that determines the importance of such system and necessary security measures to protect it.

Minimizing the risk of such problem or the scale of it requires security measures that cover all the potential initiators of the problem. Here security experts tend to differentiate 3 main categories, although some security measures are in more than one and there is no clear definition which security measure belongs where.

Physical security

For thousands of years people, goods, towns or states were protected by physical security measures starting with stone walls up to nuclear bunkers. But no matter how smart or good the defense was there were always ways to get through. Therefore combination of each category is necessary to prevent the accident.

A good example of physical security is detecting and preventing EMP weapons getting in contact with logical security measures and switching them off. A EMP blast can disable C3 (command and communication center) communication system and herewith stop the attack or prevent defensive force from operating efficiently. A good physical countermeasure may be anti air defense or air patrols in the area.

A company level physical security countermeasure may be storing information system in a shielded datacenter with UPS.

Logical security

This is the main cyber-security battlefield where digital information is being exchanged or stored. Every security measure that is performed by a non-human device in the digital world is a member of this group.

There are many sub-fields here:

- Encryption
- Network security
- System security
- Application security
- Security monitoring/auditing

Organizational security

Even if information is sealed behind the blast doors there might be a risk that somebody would open the door and let the attacker take it.

That is why security procedures are in place to ensure that in case other security measures fail people would know what to do and by following procedures ensure the safety of the information. Very often in stressful situations with lack of expertise people tend to do more mistakes than ever. Procedures are there to help people do the right thing even if they don't know what to do these guidelines would show them how to prevent the worst.

Offence

Strike scenario

The cyber-attack requires detailed structure and a plan in order to achieve the expected objective. Such plan should have this structure:

- 1.General Target analysis
- 2.Choosing specific objectives
- 3.Selection of team members with sufficient qualification
- 4.Detailed target analysis
- 5.Attack planning
- 6.Training the attack
- 7.Execution of the attack
- 8.Observing the target to ensure the objectives were met

At first point analysts collect as much information about the target as possible by standard means (eg. Newspapers, web-sites; newsgroups;..). This information should help identify:

- ⑩ Target's mission (what is the goal of system's existence)
- ⑩ Content and structure of the target's systems (network structure; geographical location; external systems connected; customers ;..)
- ⑩ Technologies used (systems used; software and hardware implemented; defensive measures)
- ⑩ History of system implementation (system integration times; upgrade dates; vendors)
- ⑩ Human resources (how many people are employed; how well trained are they; what kind of information they collect; what are their interests;..)

All the information above should help to pick up the best (or the weakest) target and possible source of attack as well as time plan of action.

Second point should identify all the weakest spots or interesting spots that should be looked into more deeply. These targets do not have to be specific systems they also can be information sources or people.

In third point the team should be assembled containing specialists for every type of system used at the target. As it is not always possible to collect all the information necessary to choose the team all the starting members in the team should be able to call in any specialists they need for target analysis or strike.

Point four should gather all the necessary information about the target to create a specific plan of action to achieve the objectives specified in point two. This point identifies specific target structure and validates the information collected at point one. This is done by scanning the target systems and identifying operation systems, network elements as well as services and daemons running on them.

At point five the above information is processed and specific weaknesses identified for possible break-in. It is not always possible to identify them up to the detail necessary, but with correlation of other information collected it may be possible to make the attack plan more specific. The plan can contain further testing and scanning as there may be other systems that are not identifiable from outside.

Training the attack at point six is a preparation for the attack that optimizes and tests the cyber-weapons as well as the plan for the attack on a group of similar systems. This also helps to develop a certain level of automation that speeds up the attack and

minimizes the probability of human intervention.

Attack plan is usually very simple:

1. use a system vulnerability detected
2. gain the authorization level required
3. achieve the objectives
4. remove all the clues (if the objective was other than destroy the target)

Verification of achieving the objectives is dependant on their contents, but can be proved by analyzing the information collected or checking the target's services that should have been disrupted or analyzing the local information sources (eg. Newspapers).

Training

Building cyber army from volunteers can't be a solution for national security even if they are the elite of computer security experts. It is the same as if best sportsmen or hunters were to build an army. They may run fast or excell in precision shooting, but they will not succeed in logistics and tactics.

In order to train a cyber army there needs to be a structure created that will use them efficiently. There have to be procedures created to help handle the situations effectively. All this needs to be built first before any training can begin.

It is already clear that standard army field manuals can't be used to help build the cyber troops as here quality matters not quantity. Also tactics has to be built from scratch in order to achieve objectives necessary. Separation of offensive and defensive training is more clearer and distinctive than in real combat training.

Defensive training

Infrastructure protection requires training in security technologies.

<i>Field</i>	<i>Technologies</i>	<i>Roles</i>
Network Security	<ul style="list-style-type: none"> ⑩ Firewalls ⑩ NIDS ⑩ Network design 	<ul style="list-style-type: none"> Firewalls specialist NIDS specialist Network designer
System Security	<ul style="list-style-type: none"> ⑩ System installation and configuration ⑩ HIDS (system monitoring, integrity checking) ⑩ Authentication ⑩ Auditing and logging ⑩ System programming 	<ul style="list-style-type: none"> ⑩ System administrator ⑩ HIDS specialist ⑩ Authentication specialist ⑩ System auditor ⑩ System coder
Application Security	<ul style="list-style-type: none"> ⑩ Application installation and configuration ⑩ Application design and development ⑩ Data encryption 	<ul style="list-style-type: none"> ⑩ Application administrator ⑩ Application developer ⑩ Encryption specialist
Organization Security	<ul style="list-style-type: none"> ⑩ Security policies ⑩ Disaster recovery planning ⑩ Incident handling ⑩ Forensics ⑩ Auditing 	<ul style="list-style-type: none"> ⑩ Policy writer ⑩ Disaster recovery planner ⑩ Incident manager ⑩ Forensics officer ⑩ Auditor
Other	<ul style="list-style-type: none"> ⑩ Security monitoring 	<ul style="list-style-type: none"> ⑩ Surveillance crew

All the roles described above are already existant in many companies and government agencies. There are many trainings for technologies specified above, but in order to use them in cyberwarfare they need to be integrated together.

For example there is a potential target detected and commanding officer decides it is important to protect the target. Here is a general plan that needs to be executed:

- 1.auditors are sent onsite to investigate current status of security
- 2.Every area specified above is assessed and commanding officer decides what area needs improvement and what experts would join the taskforce.
- 3.Experts start improvements in organizational security (priority nr.1)
- 4.After improving security policy other areas start improving systems and networks accordingly.
- 5.Incident reporting (if possible also security monitoring) is linked to a defence center with security surveillance crew.
- 6.General advisory is given to the target's security crew.

- 7.After deescalation of security alert monitoring and incident reporting is given back to target's security team.

This all needs to happen in a very short time as cyber attacks may start immediately after warning. Also cooperation with target's security team is vital due to the fact that they know their systems better.

Defence teams need to be trained in various technologies on the market and practice their skills on most of the common systems on the market.

Trainings on specific technologies need to be done by external companies who have resources and skills for it, but trainings in tactics should be done locally with cooperation of offensive warfare teams.

There are 3 types of training:

- 1.Proactive securing of a target
- 2.Immediate reaction on a attack and security of the target
- 3.Security forensics after attack and securing of target's infrastructure to prevent more attacks

Type 1 training start with deployment of a system with application and a function defined for it. It continues with performing security checklists in order to bring the system and network components to a securely configured level. Next there are active security measures deployed in order to prevent majority of standard attacks. After that there are passive security measures deployed to monitor the system as well as provide sufficient auditing data to identify what happened.

Type 2 trainings are very similar to security drills on a military base. After an alert is issued team members have to gain control over the system and remove all the attackers from the system. This can be done with cooperation with offensive warfare teams. After alert is issued there needs to be an escalation procedure executed which informs global security control center (GSC2) of an ongoing attack. After gaining back complete control of the system team has to investigate how attackers got into the system and report it to GSC2. With this information system needs to be secured and security holes need to be patched. Also this process needs to be reported to GSC2 in order to secure other similar system that may be possible targets.

Type 3 trainings take place in systems that have already been hacked. Their main objective is to analyze system state and logs and reconstruct the actions that attackers did. This can help to secure the system as well as give some information to offensive

warfare teams how to perform similar attacks. Another objective is to detect what has been changed in the system to prevent further damage or fraud.

Offensive training

It is difficult to train something not very specific that varies every moment. Offensive cyberwarfare is a set of tools and technologies based on security holes in various software. These holes get fixed very quickly and training how to misuse them would become obsolete after several days. Offensive training should be therefore based on general technologies rather than on specific tools.

Training objectives:

- ⑩ psychological fitness (working under time pressure)
- ⑩ technological understanding (general concepts of systems and networks)
- ⑩ operational procedures and policies understanding
- ⑩ State/government/army functionality understanding (information flow, command structure)

In order to meet these objectives there should be a training plan set to meet the army needs.

Psychological fitness

To succeed in cyber battlefield soldier needs to be able to work under pressure and make correct decisions very fast. Just like in conventional warfare a hole or a window in enemy's defence is opened for limited amount of time. Strike team needs to use this window and every second counts that they can gain with good preparation and training. Stress is not only a side-effect when working under pressure but also a key factor for success. Training should be done just in a same way as conventional trainings by learning procedures in order to minimize the reaction time in between.

Technological understanding

In conventional warfare it is necessary to know how weapons work in order to use them properly. This same concept is necessary for cyber-warfare. The level of detail must be sufficient to guarantee understanding of what happened, is happening or is expected to happen. By knowing the technologies a cyberwarrior is able to make decisions and predict the enemy move as human interactions are very rare to happen. Understanding of networking and operation systems technology should not be underestimated and should be the main objective of cyberwarrior's training.

Operational procedures and policies

Technological protection is very limited thanks to openness of every system. Protective measures don't affect required functionality of a system and therefore can't be expected to be the only defense of a target. By logical security there is also organizational security that comprises of procedures and policies. These are usually deployed in order to strengthen the defences up to a maximum. Due to the human nature they are not as quick and precise as technological means, but they are not very visible and can't be easily predicted.

As an example if the target follows government cybersecurity standard and has already detected a breach it needs around 10 minutes to report an incident and ask for help. This external help requires at least 30 minutes to analyze the environment and assess the indicators of the breach. All

this time can be used for achieving the objectives and covering tracks by cyberattack team.
By knowing standard procedures employed in specific industry a cyberwarrior is able to predict the human response and assess the actions necessary to take or the remaining time he has to achieve his objectives.

General target's functionality

Learning about counterforce functionality and structure helps to choose the correct targets as well as make quick decisions about tactics to be used in specific attack. By hitting correct targets it is possible to achieve expected effect as well as create sufficient confusion and distraction to enlarge the attack window or leave the attacked system unnoticed. Although it is not very useful for execution cyberforce but it is surely valuable for target choosing or tactics planning,

As an example US government initiated cyber-defence strategy which requires central emergency center. Information about the incident should be sent to the experts there but if the path is disabled and cyberattack team takes over the communication target may be gained easier under control.

Or by estimating time of response from the target knowing of existence of such center can increase the time delay of such response as target is expected to wait until the decision from such center.

Conclusion

Gaining importance of information systems in today's warfare shows that information security is being a key to success of a conflict or even a war. Cyber warfare is becoming more and more powerful on today's battlefield and affects development of armies in many countries as well as development of weapon technologies. Its use should not be underestimated as it is highly flexible and hard to detect. Its costs allow any country to train or hire a team capable of doing more than a complete army. Effective use of such teams can gain dominance on battlefield or force the enemy to retreat by shutting down its command infrastructure or communication network. Value of cyberwarfare is growing and with digitization of conventional warfare technologies as well as using more complex devices creates risks and weaknesses that allow cyberwarfare units to do more damage than they could in past.

Information age is taking over conventional industries and with growing needs for automation and digitization nations realize lack of skilled people able to control them. Governments realize that this problem is slowing economy but they don't realize that it also creates risks and holes in national security strategy. Shutting down nuclear powerplants may destroy the whole economy in a matter of minutes; opening water dams may kill thousands of people or releasing poisonous chemicals destroy country's nature.

Cyberwarfare units have a important mission to ensure country's survivability, prosperity and stability. They need to ensure national security and in worst case help with disaster recovery. In past countries relied on strength of conventional military units but now future of a country may depend on how well trained cyberwarfare units are and how much practice they have .

Enemy is already there and getting stronger every moment. We must make sure we can keep him from destroying our values we've been creating so hardly.

Appendix A. Offensive training scenario

Mission description

Intelligence reports a planned cyber-attack against powerplants and energy distribution systems. They request a ransom of \$1 000 000 or they shutdown the power grid in a big city. The enemy was located in a not friendly country and there is a suspicion that they planted an automatic attack mechanism on various places in the network.

Plan

A Cyberattack team should be sent in escorted by special forces to investigate and neutralize potential threat .

Special forces are to secure the area and neutralize any physical threats. They should ensure safety of cyberattack team and help them reaching the objectives of the training. The team should remain undetected by local authorities.

Cyberattack team should be composed of:

- ⊗forensics specialists
- ⊗firewalls specialist
- ⊗system security specialist
- ⊗specialist in energy industry's applications security

They are to collect all the information about the plan and tools used as well as investigate any external potential threats from the local connection.

Forensics specialists should be collecting any kind of evidence about the planned attack or possible future attacks as well as other information that might help increase the security of the homeland.

The rest of cyberattack team should investigate possible threats seen from the local connections available to the attack group after the forensics specialists have recovered all the information necessary.

In case they detect possible external automatic attack mechanisms the rest of the team should try to disable it and report them to the local defence teams of these external locations.

Objectives

- 1.location of external automatic attack mechanisms
- 2.elimination of detected external automatic attack mechanisms
- 3.recovery of attack software that should have been used
- 4.stay undetected by local authorities for the time necessary.

Appendix B. Example of target analysis

Commerce Department is responsible for providing timely warnings of hurricanes through its Tropical Prediction Center (the TPC) in Miami, Florida. Incapacity or destruction of this essential government service could result in considerable loss of life and property. Indeed, thousands of people died during the Galveston, Texas hurricane of 1900 because there was no advance warning of the hurricane's approach and, thus, no one evacuated the city. In 1992, Hurricane Andrew would have been even more devastating than it was had the TCP not been able to provide timely information about the storm, thereby enabling thousands to evacuate from those areas where the storm's predicted strength threatened to be greatest. Although the TPC is a critical asset, it does not operate in isolation; it depends on a variety of other government agency assets, as well as assets owned and operated by private government contractors. These include satellite imaging and analysis centers and radio transmission facilities located in Maryland and Pennsylvania. Operational disruptions at any one of these facilities could impede the delivery of timely hurricane warnings just as effectively as operational disruptions at the TPC itself. Furthermore, the TPC depends on specific providers of critical infrastructure services to operate, including Florida Power & Light for electric power, and Bell South & MC 2000 for telecommunications. Disruptions to these services also could impede TCP operations that are necessary to deliver hurricane warnings.

Effect:

- ⑩ Disable early warning system against hurricanes.
- ⑩ Damage indirectly in certain regions (with proper timing)
- ⑩ Kill people indirectly in certain regions (with proper timing)
- ⑩ Create negative image on state's government functionality (with proper timing)
- ⑩ Create confusion and minimize trust in early warning systems

Objectives

- ⑩ Disable electric power distribution
- ⑩ Disable telecommunications systems
- ⑩ Disable satellite imaging capabilities
- ⑩ Modify satellite imaging capabilities
- ⑩ Modify telecommunications systems