Autoimmune Cyber Retaliation Supported by Visual Analytics

Eng. Mihai-Gabriel IONIȚĂ, Prof. Victor-Valeriu PATRICIU
Faculty of Military Electronic and Information Systems
Military Technical Academy, Bucharest
ROMANIA
mihai_ionita01@hotmail.com, vip@mta.ro

Abstract: As the World Wide Web contains close to 500 exabytes, it is clear that securing it is a very important and difficult task. Security specialists and analysts are faced with challenges regarding the sheer quantity of data which has to be analyzed. As the quantity of data grows, automated analysis within a single piece of equipment is not feasible anymore. This is why security analysts are divided between a dozen of consoles from a dozen of pieces of equipment from different vendors, each with its own standards and rules for representing data. Unfortunately human operators cannot efficiently take decisions based on the output of a dozen consoles, each with a different data representation pattern. This is why the cognitive abilities of a human being to reason analytically have to be used. This can be offered to an operator only with the aid of an interactive visual experience on a single large console.

Key-Words: Autoimmune Defense, Cyber-Retaliation, Secure Information Exchange, Security, Visual AnalyticsIntroduction

1. Introduction

As said before, the world is constantly changing, as are armed conflicts. Wars can be very short, from full blown armed conflict to a "deactivated" nation in just a matter of minutes. The longest war in human history is actually a series of events that lasted approximately 721 years, from 92 BC until 629 AD; these are known as the Roman-Persian wars [1]. As a counter-example, the Slammer worm infected more than 90 percent of vulnerable hosts within 10 minutes [2]. As it began spreading throughout the Internet, by attacking randomly generated IP addresses, it doubled in size every 8.5 seconds. This attack started on a Saturday morning, and exploited a buffer overflow on computers running Microsoft SQL Server 2005. After three minutes it had already reached its full scanning speed of 55 million scans per second. This incident, with its element of surprise and incredible infection speed has caused "network outages and such unforeseen consequences as canceled airline flights, interference with elections, and ATM failures. [2]" And this all happened in 2002. After twelve years, just by analyzing Stuxnet or Red October someone can see the increase in sophistication of these attacks.

In that period human intervention couldn't have been possible in a timely manner. Unfortunately, not even today, given all the advanced systems deployed in computer networks or on hosts, a human reaction would not be optimal, taking into account the speed at which these operations happen. Not to mention the stealth with which they are operated.

This is why an intelligent system has to take the decision, and act accordingly, in order to terminate the threat or at least minimize its effects.

2. Modern threats

2.1 Cyber Espionage

Cyber espionage is one of the intelligence areas that got a lot easier after everybody's life and business moved online. Today's cyber stage is garnished with malware crafted for fulfilling different objectives. One objective can be stealing banking information like the Zeus trojan does.

Or, another objective can be stealing corporate data, or even sensitive, classified information, from government

ISSN 2067 – 4074

agencies computers, as is the case of the malware named Red October. Not only this, but this "weapon" could install itself on a phone, running the Windows Mobile operating system, connected to the infected computer. This was done for conversation eavesdropping, talking photos with the phone's camera, recording conversations around the phone, using its built-in microphone, searching the internal memory for documents of interest, and infecting other computers.

This malware is the typical Advanced Persistent Threat (APT). It is following the exact description of one. It is the most sophisticated cyber espionage tool ever discovered [3]. Kaspersky Lab declared that if a usual piece of new, unique malware is automatically analyzed in a few seconds; all the modules found during the Red October investigation took two months by a team of malware specialists to reverse engineer and analyze. This says only a few words regarding the level of sophistication and expertise necessary for writing such code.

As a side note, the first domain used a Command and Control server (C&C) was registered in 2007. The first evidences appeared at the middle of 2012. This means that this APT had five years for harvesting sensitive information for its creators.

If human operators had a hard time detecting the threat, how would a system performing permanent inspection of the network would [4] have performed?

2.2 Industrial sabotage

Not only cyber espionage but also industrial sabotage saw an increase in performance after everything is electronically controlled and monitored.

The greatest cyber weapon used for industrial sabotage, of all time, is the Stuxnet worm. It was written especially for incapacitating Iran's nuclear powers. It seems that it has been created by Israel and the United States of America [5]. It is an engineering masterpiece. In the way it works, in the way it was deployed for passing an air gap between networks, and the way it functions [6]. It targets a specific programmable logic controller, Siemens S7-300, found in the Natanz fuel enrichment plant. The way it spreads itself through the network, multiplying, the way it hides its actions, quickly changing the centrifuge's speed, from monitoring software, are traits that mimic those of human viruses.

If malware copies traits from the human world, why would the cyber defenses not do the same?

2.3 Distributed Denial of Service

In March 2013, Spamhaus, the non-profit spam fighting organization fell victim to the largest, ever recorded, Distributed Denial of Service (DDoS) attack.

The attack was carried by a series of botnets that started a DNS reflection and an ACK Reflection attack against it [4]. The particular important aspect of this attack is the sheer size of generated traffic: 300 Gigabits. The scale of this attack had huge implications, affecting 10 million internet users that tried surfing sites with no connection to CloudFlare or Spamhaus. This annoyance was caused by the mitigation technique that redirected the attack related traffic to other Tier-1 Internet Service Providers (ISP) in Europe [4]. The DNS Reflection attack consists in sending a request, with a spoofed source IP address, for a large DNS zone to a series of open DNS servers. The request being much smaller than the response, the computational load of the attacker is not high, so he can make several requests per second. The DNS servers will respond to the address specified as the source address, overwhelming the victim with unsolicited DNS zone responses, as depicted in Figure 1.

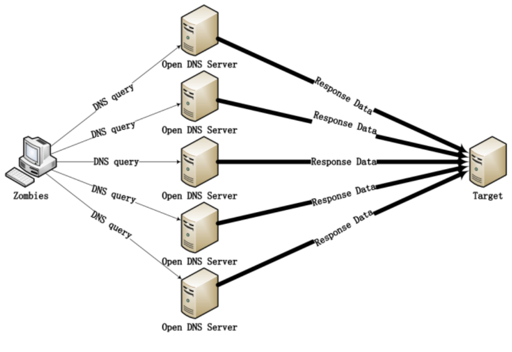

Figure 1. DNS Reflection attack description [4]

Any organization would succumb to such a fierce attack, unless suitably protected. Protection can be assured by a few ways, some better than others. The first one, used in mitigating the discussed attack consists in redirecting traffic to others. This is a good option, if the other servers could manage the load. In this case, they could not manage it, and this rerouting of traffic caused contention on other Tier1 ISPs.
The second option would be to use a top domain DNS sinkhole server that terminates useless connections.
The third and the proposed one is the use of distributed sensor servers of a Security Information and Event Management (SIEM) like defense architecture for rerouting, while load-balancing, attack related traffic to them. These would have the chance to analyze and sanitize the requests for determining if any of these are legitimate, or if anything about the attacker can be revealed. Based upon findings the reputation of those address chunks can be changed to better match their type.
This operation can be done by an autonomous defense system, which by cooperation with other similar systems around the world can identify the botnet and cease its operation in the midst of the attack.

2.4 Black market for vulnerabilities

It appears that the 0-day vulnerabilities are unknown only to the vendor of the software and its clients. These 0-day, highly exploitable, vulnerabilities are sold on the black market for sums up to 1 million dollars [7]. These vulnerabilities seem to remain unknown to the general public for up to 5 months, after which they are publicly disclosed. So, the highest bidder can have an easily exploitable vulnerability 5 months ahead of the vendor of the implicated software.
"Boutique vulnerability providers, such as VUPEN Security, ReVuln, NetraGard, Endgame Systems, and Exodus Intelligence, sell subscriptions that include 25 zero-day flaws per year for $2.5 million. Frei [7] says such pricing has cracked the monopoly of nation-states as the main customers of these bugs."
The director of cyber security of McAfee says the report [7] is a grim reminder that there are plenty of unknown threats circulating below the surface. "That's very scary," he says of the findings. "We also have to keep in mind that a lot of issues are happening in the Internet that we are not even aware of." [8]
Security wise, this approach changes the rules of the game. A system declared secure by vulnerability detection suites, which only compare different file versions to those on the assessed system, can be hacked by exploiting a 0-day vulnerability bought from the internet, that is unknown by any security testing framework.
This is why an intelligent security system has to be installed that does automated code review and vulnerability testing and learns from these actions. So it can spot, at a later time, weak points that could generate a buffer overflow, for example.

3. Architecture of the proposed autoimmune defense system

For all the problems stated in the previous section, alongside their current solutions we propose an autoimmune system based on collaborative defense techniques that mimics the action taken by the human immune system when it detects a non-self entity present inside the body. These actions include attacking the detected intruder, before it can cause more damage. This counter-attack is a very delicate one and can cause serious problems if not accorded the proper attention. The initiation of the counter-attack and the discussion of the problems it implies, alongside with the legal aspects involved will be laid out in one of the following sections.

3.1 Motivation of the system

Cyber-attacks are getting more sophisticated. Malware creators are ingenious and think of bypassing security barriers by using human beings to resolve problems for them. As is the case of the koobface malware that passes captcha security checks to the human operator in front of the screen to solve the puzzle for

it, the forwarding it back to the site that asked for it in the first place, and loging in as the unsuspecting user, with his phished or key logged credentials.
Human operators are single tasking "systems." Therefore their attention is not easily divided between different alerts. If they concentrate on a task they can easily miss an important event. So context changing is difficult or in many cases impossible without losing important information. People get sick, fall in love or have a "bad day." Computers don't fall victim to these problems. Of course, they don't posses the same reasoning capabilities as a human being, but a tradeoff has to be made. Also, we have to take into account that human beings, in a tight security operation, have to follow procedures. So the aspect of free will and reasoning that a computer system lacks begin to come short on the decision table. So, if we are able to rapidly quarantine the usual suspicious actions detected by a SIEM and minimize the damage of detected threat, all automatically without the intervention of a human operator, at the end of the day we can call it a success.
In this increasingly connected, network centric world, with concepts like the internet of things (IoT), joke aside, you can expect being swarmed by a DDOS attack coming from a number of refrigerators from Asia [9].
At the moment operation without human intervention, fully automatic operation is impossible. Firstly, because of the degraded performance it would offer and secondly, because of the undesired actions it would take, especially when it has offensive capabilities.
The offensive actions will be taken only after approval from one of the analyst teams that inspect the system's operations.
Being the last line of defense these analyst teams have presented with the most important facts of the reported incident. In this way the system will present them a graphical analysis of his findings, based upon which the team will be able to decide which actions should be taken. For this aided event presentation a visual analytics algorithm will be used to present the analyst the crucial facts in a quick and easy to understand way, similar to the one presented by Robert Rowlingson et al. in their "Visual Analytics in the Cyber Security Operations Centre" paper [10]. These techniques relieve the operator from analyzing complex data structures under pressure by using cognitive sense.

3.2 Feature description

The proposed architecture for this cyber defense system is based on the human immune system, thus it inherits its traits. First of all it has to be highly decentralized for quick action, in close proximity to the threat. But the existence of a centralized authority to which the distant reactive sensors report is useful and necessary for supervising and authorizing the sensitive actions of the decentralized agents.
In the envisioning of the architecture described in this paper, the decentralized, distant entities, called agents are the ones that have to counter-act against malware that comes in their close proximity. The action will be taken only after informing the central entity that supervises and authorizes the defensive or the offensive actions against threats. These agents are free to act, based on their own decision making process. They build decisional trees on the fly, with the obligation of reporting, in real time the actions taken to the central coordinating entity, called the root system, for journaling and traceability of actions on specific components.
Truly autonomous cyber warfare agents are not known at this time. Stuxnet is the most advanced prototype publicly known.
The first task for the agents, after detecting suspicious activity is to determine the nature of the suspicious activity and determine if the actions taken by the suspicious entity, a computer, server or application, pose a threat for the system. This determination has to be done based upon the experience of the system; also, the information from other similar systems is very important.
The root system cooperates with similar systems around it for information exchange. All this information is sanitized, checked and correlated whit the existing

information in the central knowledge repository, which is accessible to all the remote agents, for taking a decision with full awareness. Based on this correlated information, the remote agent has to determine the type of threat, once the suspicious activity has been confirmed as corresponding to a previously tagged pattern, or in correlation with information from other systems it is confirmed as a dangerous action or application.

After the threat is categorized, the event will be investigated in accordance with the attack's previously determined type.

Furthermore, to prevent unwanted surprises, any protected system suspected of being infiltrated, that could not be determined as being infected, will be forensically analyzed.

3.3 Proactive and Reactive measures taken against threats

The autonomous system discussed in this paper does the following actions to stop malware and other type of threats from spreading or, in the best case even from infiltrating the protected systems.

Architecturally the discussed system is based upon the characteristics of the human immune system. It is designed in a similar way. It has different levels of barriers for blocking attacks of different kinds. Like the human immune system has the skin as its first defensive barrier, this autoimmune system uses the defense in depth concept, based upon a series of different purpose routers that protect its separate networks.

First of all it monitors all the systems that make up the protected network, and all the connection to and from the systems of interest. This is achieved by having an OSSEC like Host Intrusion Detection System (HIDS) on every workstation, server, and protected device in general for the host log collection, behavior analysis and baseline threat status determination. For the network portion of the protected systems there are strategically placed sensors that monitor network traffic, analyzing and correlating the suspicious aspects.

All sensors involved in this traffic and behavioral analysis have artificial intelligence (AI) for coping with sophisticated attacks. These include pattern recognition and anomaly detection. The host's agents have AI algorithms based on supervised machine learning techniques, while the network sensors due to high volumes of traffic and unstructured data use unsupervised machine learning techniques. The agents face the problem of adversarial learning which makes it harder for the agent to determine an attack pattern.

As an example, against a massive spam attack, which at a national level can really cause problems, the system can deploy automatically, a DNS black list in the top level domain name servers from the nation's architecture.

If all the proactive measures fail and an infiltration or an attack is detected, than reactive measures are taken for quarantining it as quickly as possible to a single host or subnet. After the quarantine operations have succeeded, cleaning measures are taken for stopping destructive actions and resetting the security contest to its initial form.

These reactive measures are meant to be taken on systems and servers that are under control of the protected organism. They include firewall rules, on hosts, network disconnecting infected systems by shutting down access switch ports, creating domain firewall rules from preventing different data being exhilarated or malware spreading. All of these have to be done automatically for quickly stopping threats, with the information of the root component, and signaling the analyst teams.

After the threat has been contained, neutralized, and the security context returned to its normal operation, the formerly infected systems are thoroughly analyzed for any remnant infections and audited so that the system gets immunity from similar actions in the future. The audits of the result are then passed on, horizontally and vertically, to the other agents of the system for system-wide immunity against that pattern of infection.

The system will also store addressing information for all the components it analyses so they can be quickly identified.

For a system deployed at a nation level, deep packet inspection and encrypted traffic stripping has to be taken into account, with regard to the privacy issues these action arise in the public opinion. Data retention laws have to be respected for the data that is stored and processed by data mining algorithms, with the goal of finding new elements after a new match is found.

3.4 Offensive actions or active defense techniques

This identification process is done similar to the self/non-self-detection used by the human immune system to determine a biological threat. In the event that the detection process reveals a breach on any protected resource the agent announces this successful infiltration and begins by gathering information about the attacker. Determining the possible attack surface that can be exploited against the attacker in case that the decision taken, after a thorough analysis that wages the consequences, is to mount a counter attack, and the type and scale of it. A large scale attack cannot be launched solely by the artificial intelligence (AI) running on the defense system. A large scale attack can only be launched after the decision taken by the defense system's AI is approved by at least two security analysts.

The offensive capabilities of the autoimmune system, proposed in this paper, are built from the need of defending against threats described earlier in section II.

Cyber espionage and industrial sabotage are both, usually, malware related. So, if the implantation is successful, thou it should be harder, after the autonomous system is in effect, after it is detected and quarantined, it should be analyzed. After it is analyzed and every of its capabilities are checked to see if they were successful on the investigated systems, and cleaning actions were taken, the attacker has to be identified. Usually distribution methods are different, and sometimes novel, like the different methods of passing an air gap between two systems, from the obvious method of using an USB stick, to a more advanced one of using sound waves. These distribution unusual methods leave only code analysis methods as viable options. Based on different particularities of the language used, domain names, programming techniques, or hardcoded data, the system can narrow down the list for the security analyst's decision.

Against botnets, that usually cause a lot of damage by coordinated DoS attacks resulting in a DDoS frenzy that can incapacitate a large corporation, as was the example with Spamhaus or even a country, as was the case with Estonia in 2007 and Georgia in 2008, that faced severe coordinated cyber-attacks. These nationwide cyber-attacks gave birth to the threat of cyber war.

Botnets are usually composed of infected, innocent, computers, called zombies. These participate in different types of attacks, without the user knowing what his is doing while he surfs the internet. A nation, even if under attack cannot take radical measures against this type of attackers. So after rerouting traffic, on the large routers that support the worldwide internet connection, the autoimmune system will have to disinfect these zombie devices.

Traffic rerouting means integrating the ISPs in such a system or legally having the possibility to impose such actions, in case of necessity. The ISP is a critical actor, when facing an attack, from a security log sharing point of view, and also its key place in announcing actions for the public or even the attacker. The system may want to let the attacker know that he will be targeted by a retaliatory attack, to respect the law, and also for his deterrence.

This can be achieved by using a cyber-tool similar to an antivirus, based on the principles of an antibody that intervenes when an infection is present in the human body. This antiviral agent will be deployed using user contribution or exploits found after a vulnerability scan is executed. The latter option is to be used only when the first one does not work or speed is of the essence. This antiviral agent, once deployed, will scan for malware, and quarantine the initiating malevolent application. After cleaning the corrupted computer the retrieved piece of malware will be sent back to the root component

for analysis and maybe a link to the attacker.
Deciding the launch of a large scale attack is a delicate move and has to be done with great caution, and after being sure that the attacker has been successfully identified. And identifying an attacker is a very tedious process. In the present period, it can take months for an international team of code analysts to examine malware samples and determine their creators, without 100% accuracy. So, before improving this kind of attack capabilities it is very important to invest time and resources in techniques of automated code review and analysis that can give an accurate response in a matter of seconds. For high accuracy and a short time of response, developing information exchange is another key component that will be taken into discussion in the following section.
At the moment, apart from the "The Tallinn Manual on the International Law Applicable to Cyber Warfare" there are no international rules that define cyber warfare, and when a nation's act of war against another is legitimate. This is again a thorny problem that has to be taken into account when designing an autonomous system with offensive capabilities. On the interested channels there are different discussions based on this subject. The future of warfare should be built on righteous principles, because it can cause a lot of problems to the world if it is not. Unfortunately, the future of war has to be discussed because it is already here, as described is section II of these paper, involving modern threats. And a nation has to be able to protect its critical infrastructures.
Reaching true national or zonal distributed security means the cooperation of state and private actors on a network of such autoimmune interconnected and communicating systems.

4. Visual Analytics

This component becomes crucial, as said before, when the quantity of information that needs to be analyzed by a human operator exceed his capabilities. This technique is very useful in today's cyber environment where patterns have to be detected and trends have to be predicted and acted upon quickly.
This technique is based on analytical reasoning. It supports three goals: assessing, forecasting and planning in regard to the information that is being analyzed.
As in [12] analytical reasoning offers an increase in available resources when it comes to those needed in taking a decision. It reduces search times by increasing data density. It enhances the recognition of patterns. Also, it facilitates perceptual inference and monitoring.
Another fairly used technique consists in temporal visualization. Especially in the field of networking technologies, this is deployed systemically, for debugging purposes.
Video analysis is heavily used in physical security applications for detecting different intruders. Multimedia analysis helps news people easily detect important stories in the ever crowded world of television.
In complicated problems which are defined in more than 3 dimensions multivariate visualization comes in to help technicians get a grasp of the information that need to be analyzed [12].
Unfortunately, at the time of writing this paper there are not any well-defined, universally accepted metrics for classifying GUIs (graphical user interface) which employ visual analytics. This can be an interesting topic for future development of the field, as it gains attention from the public and from the key people that can sponsor it.
In this context, cyber retaliation comes in. The analyst which gives the final solution has to take a decision very quickly and in coordination with the events which take place outside his office.

4.1 Areas related to visual analytics

Basically, VA integrates Scientific and Information Visualization alongside similar disciplines like data mining, data management, human perception and cognition, and human computer interaction [13]. In our opinion the expansion of data mining was a great enabler for VA. Of course, the related discipline called Scientific Visualization emerged in the last twenty years. So it is also a young research field, as is VA.

For VA to function accordingly, the perception and cognition link has to be a sturdy one. This a multidisciplinary effort based on neurosciences, psychology and even design for creating a powerful system that can help people use their phenomenal natural perception system [13].

Human-computer interaction is anther vital part for the VA system to reach its goal of creating a working system that can really solve complex problems for human operators. It is also a multidisciplinary effort based especially on behavioral sciences.

Other development areas constitute of combinations of the basic domains which lead to the creation of niche initiatives. A few examples are spatio-temporal data, network and graph data, these being the most important to the discussed subject.

4.2 Visual analytics concepts

The largest branches in this field of technology are geospatial analysis, network analysis, temporal analysis, multimedia analysis, and multivariate visualization. These are the larger civil domains identified [12].

In the defence and military domains other concepts have emerged as maritime awareness, military intelligence, emergency management and the most important, for our paper, cyber warfare [12]. Maritime awareness is a very complex domain from the VA (visual analytics) point of view. VA is used in this case for discovering traffic patterns and for predicting ship trajectories from a maritime defence point of view. Military intelligence is one of the domains which benefits from VA, especially battlefield awareness. In this particular situation on a modern battlefield the sheer quantity of information gathered can be intimidating. Again, in the military field, a second wasted on taking a decision can mean losing a battle, or even lives. For this analysis, usually, multivariate and temporal analysis are used.

Last, but not least, cyber warfare, the initiator of many modern data mining and optimization techniques comes into discussion. The interest for attacking an enemy's cyber infrastructure was raised after all the command and control infrastructures, which facilitate central management and rapid identification of defects and errors, became connected. Now telecommunications, public utilities, SCADA systems, even traffic lights have become part of a countries cyber infrastructure. Unfortunately, the security of these systems is not top notch. And as these systems become of critical strategic importance to a country, they will have to be protected as necessary and monitored in the same fashion. As said, monitoring a national wide network of heterogeneous systems is no easy task, not even for an experienced CERT, with the necessary tools. VA get used a lot when analyzing network traffic and looking for patterns that could help a security team predict future actions of systems or users, that could lead to an attack.

5. Secure information exchange

Information exchange is one of the thorny problems in the cyber security world. Apart from the problem that very important entities, which generate a lot of traffic and suffer frequent attacks, in a community, refuse to share information because of fear of being compromised and that the peers in the information network would know too much of their internal, protected, networks.

In the modern age of cyber defense sharing correct incident information, in a timely manner, is crucial for counter-attacking all the threats. Different methods for cyber incident information sharing are proposed, accompanied by different standards and procedures. At the present time there are different enumeration types, different description languages, each with separately organized repositories. Common Vulnerabilities and Exposures (CVE), Open Web Application Security Project (OWASP), Common Attack Pattern Enumeration and Classification (CAPEC), are the major enumeration types, used selectively in different domains based on local policies and agreements. Open Vulnerability and Assessment Language (OVAL), Common Vulnerability Scoring System (CVSS), are the major description languages used within different organizations, based on the same agreements. Different repositories exist for storing and consultation of cyber event description. National Vulnerability Database (NVD), European Information Sharing and Alert System (EISAS) are national and community repositories used for synchronization of events. The first one is used by the USA, while the latter is setup by the European Union Agency for Network and Information Security (ENISA) for use in the European Union (EU).

As presented the multitude of options for sharing information makes the exchanged data, and the method itself, hard to standardize. ITU's X.1500 Cyber Security Information Exchange Framework (CYBEX) recommendations alongside NATO's Cyber Defense Data Exchange and Collaboration Infrastructure (CDXI) [11] are two of the proposals which can be used on international level for cooperation. In a similar manner the Internet Engineering Task Force (IETF) has a set of standards for cooperation: Real-time Inter-network Defense (RID) and the Incident Object Description Exchange Format (IODEF).

CDXI is one of the better documented proposals for an information sharing architecture for NATO countries. Its author [11] outlines the major problems of this domain:

"-there are no mechanisms available for automating large-scale information sharing" These are imperious in context of the proposed autoimmune system.

"-many different sources of data containing inconsistent and in some cases erroneous data exist." For an autonomous system, which processes thousands of data streams per second for taking a quick and correct decision can be the beginning of the end.

"-many protocols and access mechanisms are proprietary or not interoperable." This led to the problem in the first place, as cyber security solutions expanded and are getting more autonomous.

"-incompatible semantics using the same or similar words are used in different data sources covering the same topics." This only increases a repository size without adding any value, and making it harder for a searching algorithm or for a clustering one to provide correct results. Once again, in this context it is very important to have a clear algorithm of Quality Assurance over data received from partners.

It is important to note that this area is of great interest to the key cyber world players. And the efforts of the ITU, IETF, NATO and the MITRE Corporation by its "Making Security Measurable" in a near future will lead to an international available architecture for exchanging data in an automated, secure, verified and resilient way.

6. Conclusion

Cyber security has to be treated systemically, like the human immune system. Communication between nations, friend or foe, and different allied systems is critical for the success of any mission.

Even when designing and deploying an autoimmune system like the one described here, privacy concerns and national laws have to be programed inside it. Because this one will not only act on probabilities and preconfigured routines, but, using its AI, will also act on past experience and behavioral information. The purpose of such a system has to be its capacity of protecting citizens and governmental structures form cyber-attacks.

All the offensive actions listed here, as capabilities of the designed system are thought of as responses to the so called kinetic cyber-attacks [6]. These types of attacks have a large scope, from industrial sabotage to SCADA systems, automobiles, Building Management Systems (BMS), and even medical implants. These types of attacks are not any more merely computer, cyber-attacks; these types of attacks have the possibility to kill people if successful. This is the motivation of this design.

The author is currently implementing an early warning system based on the architecture described in this paper with a neural network as its central AI component.
Nonetheless visual analytics will become a crucial component for any serious cyber security awareness and defence tool. Important steps are taken towards creating a set of rules for definig common importance measurements for these kind of systems.

Acknowledgement

Parts of this research have been published in the Proceedings of the 7th International Conference on Security for Information Technology and Communications, SECITC 2014

References

[1] Wikipedia. Wikipedia. Roman–Persian Wars. [Online] January 6, 2014. https://en.wikipedia.org/wiki/Roman%E2%80%93Persian_Wars.
[2] Moore, David, et al., et al. The Spread of the Sapphire/Slammer Worm. CAIDA.org. [Online] http://www.caida.org/publications/papers/2003/sapphire/sapphire.html.
[3] Kaspersky Lab. "Red October" Diplomatic Cyber Attacks Investigation. Securelist. [Online] https://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation.
[4] NSFOCUS. Analysis of DDoS Attacks on Spamhaus and recommended solution. [Online] http://en.nsfocus.com/SecurityView/Analysis%20of%20DDoS%20Attacks%20on%20Spamhaus%20and%20recommended%20solution-EN-20130510.pdf.
[5] Obama Order Sped Up Wave of Cyberattacks Against Iran. The New York Times. [Online] http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=2&_r=1&seid=auto&smid=tw-nytimespolitics&pagewanted=all.
[6]. The Dawn of Kinetic Cyber. Applegate, Scott D: NATO CCD COE, 2013.
[7] Frei, Stefan. The Known Unknowns: NSS Labs, 2013. ANALYST BRIEF.
[8] Higgins, Kelly Jackson. Hacking The Zero-Day Vulnerability Market. Dark Reading. [Online] December 9, 2013. http://www.darkreading.com/vulnerability/hacking-the-zero-day-vulnerability-marke/240164591.
[9] Proofpoint. Proofpoint Uncovers Internet of Things (IoT) Cyberattack. Proofpoint. [Online] January 16, 2014. http://www.proofpoint.com/about-us/press-releases/01162014.php.
[10] Visual Analytics in the Cyber Security Operations Centre. Dr Rowlingson, Robert, et al.: IST-116 Symposium on Visual Analytics, 2013. STO-MP-IST-116.
[11] Dandurand, Luc and Serrano Serrano, Oscar. Towards Improved Cyber Security Information Sharing. NATO CCD COE Publications. 2013 5th International Conference on Cyber Conflict, 2013.
[12] Valérie Lavigne and Denis Gouin. Applicability of Visual Analytics to Defence and Security Operations. 16th Research and Technology Symposium International Command and Control “Collective C2 in Multinational Civil-Military Operations”
[13] Daniel Keim, Gennady Andrienko, Jean-Daniel Fekete, Carsten Gorg, Jorn Kohlhammer, and Guy Melanlacon .Visual Analytics: Definition, Process, and Challenges. : Information Visualization, LNCS 4950, pp. 154–175, 2008. Springer-Verlag Berlin Heidelberg 2008