2011 3rd International Conference on Cyber Conflict
C. Czosseck, E. Tyugu, T. Wingfield (Eds.)
Tallinn, Estonia, 2011 © CCD COE Publications

Requirements for a Future EWS – Cyber Defence in the Internet of the Future

Mario Golling and Björn Stelte
Universität der Bundeswehr
Faculty of Computer Science
D-85577 Neubiberg, Germany
Email: {mario.golling and bjoern.stelte}@unibw.de

***Abstract*- The emergence of new technologies and services as well as trillions of devices and petabytes of data to be processed and transferred in the Internet of the Future mean that we have to deal with new threats and vulnerabilities, in addition to handle the remaining old ones. Together with the rise of Cyber Warfare and the resulting impact on the environment means that we have to bring intelligence back to the network. Consequently, effective Cyber Defence will be more and more important. In this paper we will show that the proposed requirements for an Early Warning System are a main part of future Cyber Defence. Special attention is given on the challenges associated to the generation of early warning systems for future attacks on the Internet of the Future. The term Cyber War is used frequently but unfortunately with different intends. Therefore, we start with a definition of the term Cyber War focusing on security aspects related to the Internet of the Future, followed by an exemplification of a Cyber War, of its implications and the challenges associated to it. Then we proceed with an analysis of state of the art recent work that has been proposed on the topic. Additionally the weaknesses of these analyzed systems and approaches are presented. Finally we propose guidelines and requirements for future work which will be needed to implement a next generation early warning system for securing the Internet of the Future.**

Keywords: Cyber Defence, Cyber Warfare, Internet of the Future, Early Warning System

I. INTRODUCTION

Although it is not exactly known how the Internet of the Future will look like, some challenges are quite obvious. Cloud computing allows that data and services are provided somewhere in the network; the Internet of Things indicates an enormous amount of devices to be managed as well as data to be processed; privacy requires that a high amount of packets (payload) needs to be encrypted; Security management demands to develop concepts to assure trustworthiness and manage the security capabilities consistently according agreed security policies in the future.

Not only the Internet will change significantly, also attacks on the Internet will change dramatically. In the last years Cyber Attacks became more and more visible [1]. It's generally acknowledged that the amount of these Cyber Attacks will continue to increase. Beside of the number of attacks also the impact of future Cyber Attacks are more harmful. Over the past few years more and more mission critical devices like critical infrastructures [2] are accessible within the Internet and the people behind the attacks are more skilled then before. Of these people a huge amount is professional trained on Cyber Warfare, like the U.S. Cyber Command. It's not surprising that many nations establish cyber commands because future acts of war will also have an impact on the Internet. Warfare is shifting more and more from the traditional battlefield into the digital battlefield. Consequently, Cyber Defence is essential for every nation. Due to the distributed nature of the Internet a Cyber Attack will almost never attack only one nation. Therefore, a cooperative defence strategy is needed to thwart the impact of the attack.
Traditionally Internet providers are using Early Warning Systems (EWS) to protect themselves against and quickly react on certain Cyber Attacks. Due to a new level of cyber threats we need an improved EWS architecture with the requirement not to be limited to the borders of different providers, based on traditional packet inspection, but to gather, analyze and correlate available (network) data (e.g. flows) to detect, analyze and react to threat patterns in near real time. This includes the development of completely new approaches such as the development of virtual sensors, sophisticated correlation of data, new reasoning models for network behavior analysis, learning algorithms as well as concepts to deal with scalability, dependability and resilience, especially in IPv6 networks.

II. DEFINITION OF TERMS

Before going deeper into descriptions about principles and patterns of Cyber Wars, we define the terms used within this publication. In comparison to kinetic warfare, which we define as warfare practiced in the "real world" by all the tanks, ships, planes and soldiers of current militarizes, we like to define Cyber Warfare based on the two definitions of John Arquilla/David Ronfeldt [3] and Richard A. Clarke/Robert Knake [4] as follows:
Cyber Warfare is the unauthorized conducting of a penetration - including the preparation - by, on behalf of, or in support of, a government into another nations's computer or network, or any other activity affecting a computer system, in which the purpose is to add, alter, falsify or delete data, or cause the disruption of or damage to a computer or network, or the objects a computer system controls (such as SCADA-systems "supervisory control and data acquisition").
In contrast to classical Cyber Attacks, where the intentions are almost similarly, the implications of a Cyber War are highly relevant, because attacking a nation - and in consequence attacking the critical infrastructure of a nation - creates a higher impact and is most likely not limited to the borderline of that nation.
Following the ideas of Clausewitz on war [5] (who saw the war primarily as a clash between nations) the sophisticated threat level of Cyber War is not individuals or companies, it is one or more nations.

III. DEFINITION OF TERMS

A. *Motivation*

For a better understanding of the concepts of Cyber Wars and the connection to our topic, we like to quickly illustrate the Cyber Assault against Estonia in 2007 [6], [7], [8]. During the night of 26 April to 27 April 2007, now known as Bronze Night, riots broke out in the Estonian capital Tallinn after the Estonian government moved the Bronze Soldier - a memorial statue honoring Soviet World War II war dead - from the central square of Tallinn, to a cemetery on the city's outskirts. The move also ignited nationalist responses in the Moscow media. Simultaneously, the conflict moved into cyberspace.

The attacks began on April 27. On Russian language Internet forums, Estonian officials say, instructions were posted on how to disable government Web sites by overwhelming them with traffic, a tactic known as a denial of service attack. Most of the attacks were Internet Control Message Protocol (ICMP) floods lasting 10 hours or more. The Web sites of the Estonian president, the prime minister, Parliament and government ministries were quickly swamped with traffic, shutting them down. Hackers defaced other sites, putting, for instance, a Hitler mustache on the picture of Prime Minister Andrus Ansip on his political party's Web site. The assault continued through the weekend.

By April 30, new targets, including media Web sites, came under attack from electronic cudgels known as botnets. Roughly 1 million unwitting computers worldwide were employed. Officials said they traced bots to countries as dissimilar as the United States, China, Vietnam, Egypt and Peru.

By May 1, Estonian Internet service providers had come under sustained attack.

On May 9 a new wave of attacks began at midnight Moscow time. By his account, 4 million packets of data per second, every second for 24 hours, bombarded a host of targets that day.

By May 10, bots were probing for weaknesses in Estonian banks and especially in credit-card verification systems. They forced Estonia's largest bank to shut down online services for all customers for an hour and a half.

In the end, Estonia was unable to effectively counter the attack. It cut its Internet connections to the outside world so that people within Estonia could continue to use their conventional services.

B. *Patterns of a Cyber War*

Although other Cyber Wars, like for instance the so called Cyber War 2.0 (Russia vs. Georgia), differ in detail (first and foremost by the correlation between Cyber War and traditional "Kinetic War"; "standalone Cyber War" in Web War 1 vs. Cyber War parallel to Kinetic War at Cyber War 2.0 1), the following general patterns of a Cyber War can be identified:

1) Cyber Espionage

First in every war - as Sun Tzu puts it - 'you need to know your enemy and yourself'. Long before the actual Cyber Attack, usually done through a long period

of time, you need to obtain as many secrets as possible from your opponent (for example done with social network analysis, sniffering, conventional spies etc.).
With regard to Cyber War in Estonia, the attackers need to know potential targets (like for instance the web address of the Parliament and government, important Estonian banks and their credit-card verification systems etc.).

2) Preparation of the battlefield

Still within peacetime and after you know your opponents strength and weaknesses, it's time to prepare the battlefield. Once you made the decision, to go on war (even if you need to do it only potentionally), it's time to bring the troops in a good initial setting. In the case of Cyber War it's also time to choose new weapons. This usually comprises not only port-scans, placement of logic bombs or trapdoors etc. but also new kinds of weapons. Stuxnet is a good example for these new and highly specialized weapons targeting on specific industrial equipment [9].
Concerning the example above, attackers need to (i) know the versions of the web-servers and potential exploits in order to do the defacing of the web-site (ii) have the ability to use a Botnet during the war-time or (iii) know weaknesses in Estonian banks and credit-card verification systems etc.

3) Cyber Attack

Now it's time for the "*hot Cyber War*". Like in traditional, kinetic wars, strategy and especially the timing can be crucial. A good timing will obviously have a positive effect on the attack results. The defender will always try to limited attack opportunities and thus defend attacked services with the aim to finally win the Cyber War. This goal is hard to achieve since quick results are difficult to accomplish. The defender will try to win time thus the attacker has to consume more and more resources to continue his Cyber War attack.
In terms of our example, the first targets were governmental Web sites, followed by online news portals and ISPs and finally financial services. In the end Estonia had to cut down their Internet access to the rest of the world. This extreme action which was needed to defend the Cyber Attack shows that such an attack may have an extreme impact on the Internet connectivity of a whole region.
Several defence actions are possible, in the next section will discuss these defence opportunities.

IV. CYBER DEFENCE

When it goes to defence, one of the basic cornerstones, before making a decision, especially when it goes to distributed collaboration, is the *situational awareness*.
The term situational awareness is used frequently in computer science, further we will use the following definition:
"The perception of the elements in the environment within a volume of time and space, the comprehensions of their meaning, and the projection of their status in the near future" [10], [11].
In analogy to chess: Before you can perform a reasonable turn, you need to know the position of (preferably) all chessmen. Without a clear understanding of the current situation, you are not able to choose the winning strategy.

With regard to Cyber War, situational awareness gives answers to questions like:

- Is a Cyber War taking place right now/about do begin (when?)
- Who is attacking?
- What is being attacked?
- What kinds of methods are used for the attack?
- etc.

The sooner an attack (or the intention of an attack) is detected, the better are the defence instruments (more time to identify the real attacker, less systems affected, less blurred traces ...). But to achieve situational awareness in the area of Cyber War is not as easy as it sounds. Up to now, detecting whether a nation is engaging in *Cyber Espionage* (step 1) or *Preparing the battlefield* (step 2) is close to impossible (mainly because of the long period of time in which the actions are taken) [4]. Even within the third step, *the Cyber Attack*, simple things like attack paths or the actual attackers are hardly recognized or identified. Situational awareness in the field of Cyber War is still not sufficiently solved and an open research problem.
Referring to this, John Arquilla has argued that:
Cyber War is like Carl Sandburg's fog. It comes in on little cat feet, and it's hardly noticed. [12].
It's time to close this gap. We need to be able to inform of a future danger in order to prepare for the danger and act accordingly to mitigate or avoid it. That's why so-called EWS are - especially in the field of Cyber Defence - of very high importance.

V. IMPORTANCE OF EARLY WARNING SYSTEMS ON CYBER DEFENCE

The increasing importance of EWS is manifested in the enormous number of various research initiatives around the world such as GENI and FIND in USA, FIRE, OneLab, AutoI in Europe, NWGN in Japan, and FIF in Korea. Trillions of devices, petabytes of data, gigabytes of transfer speed, payload of packets encrypted, IPv6 as well as the virtualization of services and data impose high requirements on developing a proactive action of the Internet of the Future. Key challenges in such a highly complex environment where data and services are also located somewhere in "clouds" are *security, privacy and trust* [13].
Traditional network-based intrusion detection or intrusion prevention approaches cannot cope with such challenges. The need to protect the infrastructure of the Internet of the Future, as well as to manage such a security infrastructure has to have the highest priority. As stated by ENISA (European Network and Information Security Agency [14]), privacy and trust in a network world are already nowadays the basis for using the Internet for business, communications, social networking etc. In the Internet of the Future, where (i) all devices communicate among each other, (ii) a seamless integration of networks enables the end user to "see" only

"one network", (iii) the data and services are located or are provided somewhere in the "cloud", security, trust and privacy is needed. As traditional approaches are not sufficient any more, we need something completely new to proactively protect the infrastructure of the Internet of the Future and manage these security mechanisms in a consistent manner. More precisely, it is necessary to address the following research issues:
If we assume that the payload of packets will be encrypted because of privacy and security requirements, and also because of the huge amount of data flows, it is not possible to perform deep packet inspection. Therefore, the question that arises is what data features are exploitable for detecting an attack or a deviation from the normal network behavior?
The resulting objectives are therefore:

- An analysis and evaluation of available data (e.g. flow information, sensor data), according to developed evaluation criteria and with respect to the relevance to detect a potential attack resp. a deviation of normal behavior. Hereby an analysis of passive and active measurement techniques and possibilities is necessary in addition to the relevance of the available data.
- Development and application of correlation techniques (e.g., temporal correlation, topological correlation) of various data sources, development and application of AI approaches.
- Development of methods for trend analysis in risk management.
- Modeling of network behavior, identification of the deviation from "normal" behavior.
- Determine EWS data sharing.
- Cooperative behavior, EWS have to be able to form binding commitments.

If we assume that data and services will be located, resp. provided in "clouds", then the architecture of an EWS must address this virtualization aspect. Thus, virtualized security architecture is needed. Although virtualization is a mainstream technology nowadays, it seems that security issues are often an afterthought. Existing security models and practices cannot be directly applied to a vastly different environment. Furthermore, virtualization principles could change drastically the way we do security, that forces to rethink how to manage these security items. If we assume a pervasive environment, it is necessary to develop and adapt machine learning techniques to cope with new challenges and the changing environment.
The *objectives* of an EWS are (i) to protect next-generation networks by developing a *sophisticated next-generation EWS*, (ii) to develop novel architectures, sophisticated models for network behavioral analysis and learning algorithms in order to build the next-generation EWS, able to deal with specifics such as encrypted payload of packets, trillions of devices and petabytes of data as well as IPv6 networks, and (iii) to develop approaches and models to define "normal" behavior and anomalies, threat levels, EWS data sharing. Finally raising

management aspects have to be solved taking latest overall security management initiatives in mind [15].
Key elements can be summarized as follows:

- Protect next-generation networks by developing a *sophisticated next-generation EWS*
- Develop novel architectures, sophisticated models for network behavioral analysis and learning algorithms in order to build the next-generation European EWS system, able to deal with specifics such as encrypted payload of packets, trillions of devices and petabytes of data as well as IPv6 networks
- Develop sophisticated correlation approaches to analyze, correlate and evaluate existing data (e.g. flow information), and to reason about threat levels on basis of existing data; develop novel methods of detecting malware-driven network beaconing and command & control channels using both temporal and spatial flow attributes; develop concepts of fuzzy searching for resilient and adaptable malware detection at various sensing points in the network; investigate techniques for interpreting distributed sensor data for broader situational awareness
- Fundamentally improve the state-of-the-art in automated network threat blacklist derivation
- Develop approaches and models to define "normal" behavior and anomalies, threat levels, EWS data sharing; improve the automated assimilation of new security advisories and early warnings
- Improve the understanding of virtualization security (e.g., virtual sensors), develop new security models

Based on the requirements, we have evaluated current approaches and in the next section, we give a comparison of the different technologies.

VI. OVERVIEW OF EXISTING SYSTEMS AND APPROACHES

Currently, two fundamental techniques are used for network-based intrusion detection: misuse detection and anomaly detection.
The first one encompasses the signature based group of systems. There, the detection is accomplished by the definition of malicious behavior i.e. by a set of patterns saved in advanced and discarded in a database for example. The traffic is checked for the presence of a previously known pattern either by testing the whole packet including the payload or by simply checking the header. This is the most common type of intrusion detection system (IDS) and widely in use. Especially in an environment with very high bandwidth it is not possible to inspect the complete payload because of the amount of processing power needed. Some approaches try to overcome these restrictions by applying machine learning techniques to achieve a complete payload inspection with bandwidth over 1 Gbps, for example the project ReMIND from Fraunhofer [16].

Systems that are based on anomaly detection construct a behavioral model that describes the positive behavior, thus the types, amounts, daily traffic allocation, etc. of the monitored network. The detection is realized by the measurement of the current state of the system and the comparison to the values gained from the model. Therefore, machine learning techniques are used, such as expert systems, data mining algorithms, evolutionary algorithms, and neural networks.
Also combinations are possible, for example the application of Evolutionary Algorithms in Data Mining Systems. This type of IDS is also called Network Behavioral Analysis (NBA). An enhancement of NBA systems is called Network Situation Awareness (NSA), where visualization and high-level data management are included to the process of network monitoring.
The main challenges for the protection of the network and the detection of malicious traffic and behavior comprise among other things are data and alarm correlation, source determination and forensic capabilities.
Current techniques to address these requirements are routers as honeypots, DDoS detection with honeypots, traffic diversion to honeyfarms, other information sources (like system, security and network capture/trace data), usage of protocols (like BGP, MPLS, Netflow, etc.), and usage of the human eye to catch anomalies. Due to increasing bandwidth and increasing number of services, the current systems are already hardly able to keep up with the development, and further systems will not be manageable anymore.
In the next section we will shortly describe the work of related projects. These projects try to find solutions for current Internet-related problems; early warning systems especially focusing on security aspects of the Internet of the Future.

A. *Early Warning and Intrusion Detection based on Combined AI Methods*

The project Early Warning and Intrusion Detection System Based on Combined AI Methods (FIDeS) funded by the German Ministry of Research and Education (BMBF) aims at developing an advanced, intelligent assistance system for detecting attacks from the Internet both in local area networks and in wide area networks as early as possible [18]. Within the framework, widely-used Internet protocols such as FTP, SMTP, and HTTP shall be considered, but also newer protocols such as SOAP. In addition, fraudulent access in security-critical, IT-based business processes of enterprises will be detected. Conventional IDS and in particular IDS for anomaly detection usually produce a high false positive rate or do not detect all attacks (false negatives). Complementary to anomaly-based IDS, the project develops an early warning system based upon using different methods of Artificial Intelligence (AI). This system supports a security officer in analyzing attacks and carrying out appropriate counter measures. Consequently, the project FIDeS focuses more on assistance (such as concrete instructions in case of an attack) rather than on mere intrusion detection. For this purpose, various AI-based methods are used such as declarative knowledge representation, the generation of explanations, and cognitive assistance.

B. *Event Monitoring Enabling Responses to Anomalous Live Disturbances (EMERALD)*

The EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbances) environment is a distributed scalable tool suite for tracking malicious activity through and across large networks [19]. EMERALD introduces a highly distributed, building-block approach to network surveillance, attack isolation, and automated response. It combines models from research in distributed high-volume event correlation methodologies with over a decade of intrusion detection research and engineering experience. The approach is novel in its use of highly distributed, independently tunable, surveillance and response monitors that are deployable polymorphically at various abstract layers in a large network.

C. *ARAKIS*

ARAKIS [20] is a nationwide, near real-time, network security event early warning system developed by NASK and operated by CERT Polskai [21]. The system consists of a central repository and distributed sensors that collect and correlate data from different sources including low-interaction honeypots, firewalls, anti-virus systems and darknets. The system is oriented towards detection and characterization of new attacks based on the automated analysis of captured honeypot payloads and supporting data. Further information can be found at [21].

D. *WOMBAT – Worldwide Observatory of Malicious Behaviors and Attack Threats*

WOMBAT is an European project (STREP) under the FP7 ICTWork Program 2007–08 Objective 1.4 [22]. The project aims at providing new means to understand the existing and emerging threats that are targeting the Internet economy and the net citizens. To reach this goal, the project is structured around the three following main objectives:

1) *Real time gathering of a diverse set of security related raw data*
2) *Data enrichment by means of various analysis techniques*
3) *Threats Analysis*

The acquired knowledge will be shared with all interested security actors (ISPs, CERTs, security vendors, etc.), enabling them to make sound security investment decisions and to focus on the most dangerous activities first. The project also aims to increase the level of confidence of European citizens into the net economy. Project results and innovation are new data gathering tools, advanced features (high interaction, real-time analysis), new targets (802.11p (car-to-x), bluetooth, RFID, etc.), tools and techniques for characterization of malware, and malware-based analysis and contextual analysis.
The WOMBAT project has shown so far that the generation of good benchmarks for malware detection techniques is a challenging problem, especially:

- Amount and dynamics of nowadays malware makes the generation of an exhaustive sample set an almost impossible task
- Importance of filtering samples to spot cases that could potentially lead to ambiguities
- Problem of labeling: how to define whether the label assigned to a sample is correct?

VII. WEAKNESSES OF THE CURRENT APPROACHES

Although there are some components which try to monitor the status of the Internet and to detect new threats and network anomalies; these systems suffer from the following shortcomings:

- Internet telescopes and monitoring systems **strongly rely on the use of the dark address space**. Although this is efficient for the detection of worms, network scans, etc., target-oriented attacks are hard to be recognized [23].
- Misuse detection is realized in particular by means of **Deep Packet Inspection (DPI)** and the evaluation of header information. DPI does not scale well with massive bandwidth levels, such as those at the Internet backbone [24].
- One of the most important sources for information is the evaluation of **flow data**. All of the systems in use strongly rely on the evaluation of sFlow which is a sampling technology and therefore not able to provide 100% accurate results [25].
- Early Warning Systems only evaluate **logs, flows** or are realized by **packet counting** [26].
- The inherent division between network and host-based indicators is a weakness of the current approaches. Currently, there is no robust system known that **effectively correlate** these disparate data streams [27].
- **Anomaly detection** is only realized **in subnets** and it is extremely difficult to profile "normal" behavior with any level of identity [24].
- The operation on an **inhomogeneous and non-interoperable** security infrastructure, containing stovepipe systems, and application- and task-specific "security silos" is a shortcoming of state of the art approaches [28].

In the context of the Internet of the Future, the difficulties to adapt these systems are even worse because of the changing characteristics (illustrated in Figure 1). An overview of the requirements for current approaches is given in Table I.

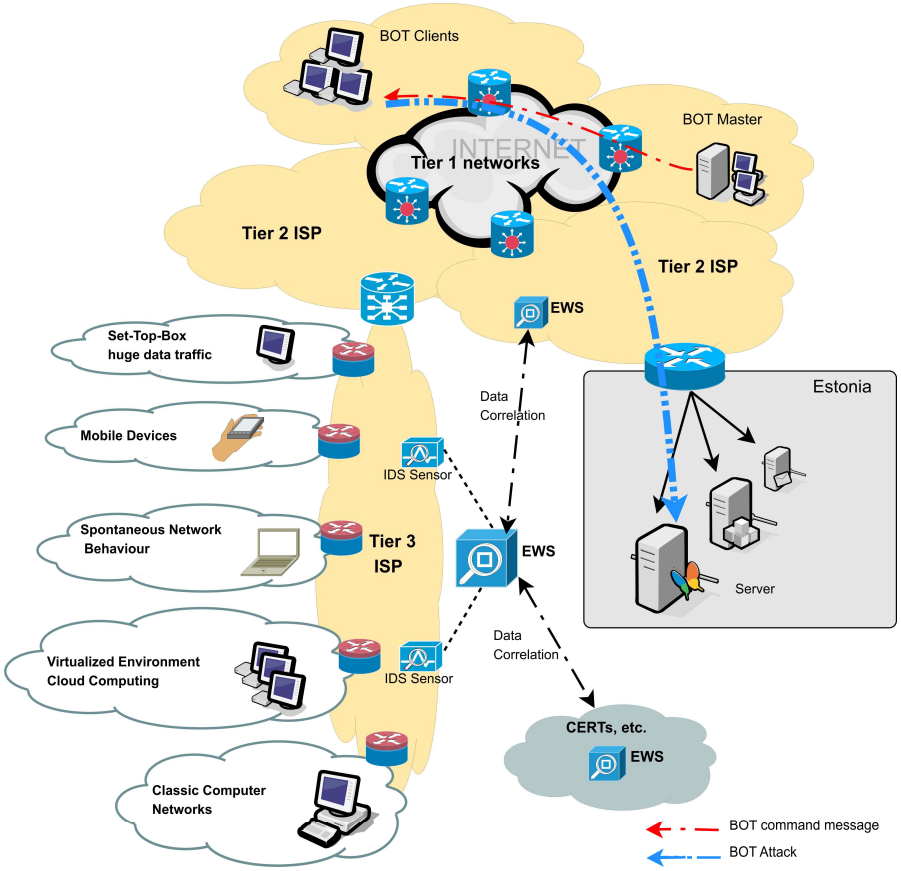

FIGURE I CHALLENGES FOR FUTURE EWS TECHNOLOGIES

TABLE I CAPABILITIES OF STATE-OF-THE-ART EWS TECHNOLOGIES

Requirements	Misuse Detection	Anomaly Detection	NEWS plugin [36]	A-EWS [17]	SANS ISC [37]	ATLAS threat index [38]	FIDeS [18]	EMERALD [19]	ARAKIS [20]	WOMBAT [22]
Extended Flow Handling	X									
Sophisticated Correlation of data				(X)			(X)	(X)		(X)
Comprehensive Reasoning Model										
Traffic Volume Independency	X	X		X	X	X	X	X	X	(X)
End-System Independency	X	X		X	X	X	X	X	X	(X)
Payload-independent analysis		(X)	(X)	(X)						
Safeguarding Mobile Devices										
Virtualized Environment / Clouds	X									
Spontaneous Network behavior										

Thus, the following requirements have to be fulfilled:

- **Extended Flow Handling:** As proposed by CISCO Visual Networking Index the global mobile data traffic will increase 26-fold between 2010 and 2015 reaching 6.3 Exabyte per month [29], [30]. Also, CISCO assumes that global IP traffic will exceed to about 767 Exabyte from 2009 to 2014. Traditional signature based approaches are not sufficient to that global IP traffic. Obviously, efficient signature flow solutions are needed in future EWS. Thus, extended flow handling is required to detect malicious traffic in the future [31].

- **Sophisticated Correlation of data**: Not only data collection algorithms are required, without data correlation an EWS will be unable to detect events. In future networks different data sources (internal IDS, ISP-CERT, national CERT, etc.) have to be analyzed with different analysis methods (signature, anomaly, etc.). Thus, a sophisticated correlation of data of different sources and methods is a requirement for an EWS [32].

- **Comprehensive Reasoning Model**: Current approaches used in intrusion detection systems are based on the traditional views of computer security. An alternative view that may provide better security systems is based on adopting the design principles from the natural immune systems, which in essence solve similar types of problems in living organisms [33]. Artificial immunology concepts for handling intrusion detection through approximate reasoning have to be used in future EWS.

- **Traffic Volume Independency & End-System Independency**: Scalability, such as independency of data traffic is needed to sufficiently detect intrusions in huge computer networks. Detecting malicious network behavior should be independent from IP traffic generated by different end-systems.

- **Payload-independent analysis:** In future networks the amount of connected devices will increase dramatically [34] next to global data traffic [29], [30]. Payload analysis may not influence the EWS detection of malicious traffic.

- **Safeguarding Mobile Devices**: The amount of global data traffic from mobile device will continue to increase significantly [30]. Future EWS have to be aware of mobile data traffic.

- **Virtualized Environment / Clouds**: Currently the usage of cloud services are widely discussed, in the near future cloud services will be largely used. On the one hand future EWS could benefit from this concept by usage of cloud services on the other hand EWS have to cope with new kind of attacks on these new services.

- **Spontaneous Network behavior**: As proposed by CISCO the number of mobile device will increase and therefore the proportion of ad hoc based traffic will increase in the following years [30], [35]. Therefore, future EWS have to cope with spontaneous network behavior.

VIII. EARLY WARNING IN THE FUTURE

The inter-relationships and inter-dependencies between formerly stand-alone systems and networks are leading to complexities in the infrastructures of our society that have never been seen before. These complex systems and networks disseminate and process massive amounts of personal and business data, information and content in ways which are difficult to understand and control for users, in particular private citizens. In recent years we have witnessed a growing series of accidents and attacks on the Internet and on applications and databases. Through denial of service attacks, viruses, phishing, spyware and other malware, criminals disrupt service provisioning and steal personal or confidential business data for financial gain or other purposes. An increasingly organized and efficient though disruptive e-market is thus taking shape on an international scale. Although we do not know how the Internet of the Future will look like, some characteristics can be identified:

- Layered, but augmented by a number of cross-cutting dependencies.
- Multitude in scale compared to the current Internet, billions of entities including things.
- Spontaneous and emerging behaviors and unanticipated new usages.
- Trust, privacy and security as key components.
- Pervasive digital environment, heterogeneous infrastructures, terminals and technologies.
- User-centricity and usability is critical.
- Enabling the "Internet of Services" and its new business models.
- Trust, privacy and security as key components, managed according a common security policy.

In respect to these characteristics the aim of our requirements is the development of an efficient cooperative Early Warning System for future networks.
In the current environment of the Internet, multiple distributed and heterogeneous networks are connected at which no encryption is done or mostly only partial. Security-related cooperation between autonomous system providers is only done on a very marginal level. Anomaly detection, which is a very powerful instrument for intrusion detection, is only possible and available for subnetworks, while current EWS are based on the analysis of log-files, flow-information or packet counting. Characteristics of the Future Internet will include a virtualized environment, IPv6 network, continuous payload encryption, an enormous number of devices and data as well as a highly distributed and pervasive environment. Therefore, most of the current components and management approaches are not applicable or sufficient any longer. To overcome these shortcomings, an efficient EWS has to be based on a network virtualization and will implement an EWS based on the use of virtual sensors, new reasoning models, new developed learning

algorithms and a sophisticated correlation of data also taking into account security management aspects.
A long-overdue EWS will help the region to avoid deliberate or inadvertent outages, reduce the spread of new computer malware, and ensure continuity of services. Furthermore, the Future Internet has no centralized control hub and its complexity is not bounded by geographical, political, administrative or cultural borders. EWSs are present in various systems and are a crucial component of effective risk management in enterprises and for national homeland security systems. An Internet-wide EWS however is still missing.
Because of the identified characteristics of the Internet of the Future, an EWS has to overcome the following issues that make the use of current State-of-the-Art Intrusion Detection Systems impossible or disadvantageous:

- **Applicability**: The **persistent payload encryption** blights Deep Packet Inspection.
- **Computational effort**: High bandwidth, numerous, **highly dynamic connections and huge amounts of data** would necessitate enormous amounts of computational power for deploying traditional systems and algorithms.
- **Energy consumption**: Mobile devices are becoming more and more important and the mobility will be one of the main characteristics of the Future Internet. Because of the increasing complexity of mobile applications, the processing capabilities of the mobile hardware and the endurance of the battery, it is neither possible nor desirable to set up sophisticated IDS on these devices. Therefore, the protection of the whole network from inside out is necessary and thus the **intelligence has to be brought back to the network**.
- **Novel threats: threats and attack possibilities** evolving from the highly dynamic environment with billions of devices cannot be handled by current systems, are not even known today.

IX. CONCLUSIONS

The Internet of the Future will consist of dynamically scalable and virtualized resources, which will be provided by providers as a service over the Internet. Due to the fact that the number of "services over the Internet" will increase tremendously and get more and more important as new business models, the providers of the Internet of the Future will need to cope with new problems.
The emergence of new technologies and services as well as trillions of devices and petabytes of data to be processed and transferred mean that we have to deal with new threats and vulnerabilities, in addition to handle the remaining old ones. They have to cope with attacks on their network, but their well-established *Intrusion Detection Systems* (IDS) and *Early Warning Systems* (EWS) will not defend them anymore, because the packet payload will be encrypted. As all current IDS and EWS installed by the providers rely on analyzing the packet payload or packet

headers to proper fulfill their tasks, we need a new kind of EWS suitable for the needs of future computer networks.

In this paper we have evaluated requirements needed to be fulfilled by an enhanced Early Warning System which is able to inform about ongoing Cyber Attacks. As shown in an analysis, so far no system can completely comply with the requirements presented. An efficient Cyber Defence is only promising if and only if the capabilities and the requirements are congruent as much as possible. Therefore, further research activities are needed in the future to build such enhanced EWS [39].

ACKNOWLEDGMENT

The authors wish to thank the members of the Chair for Communication Systems and Internet Services at the Universität der Bundeswehr München, headed by Prof. Dr. Gabi Dreo Rodosek, for helpful discussions and valuable comments on previous versions of this paper. The Chair is part of the Munich Network Management Team.

REFERENCES

[1] M. Libicki, Cyberdeterrence and Cyberwar. Rand Corporation, 2009.

[2] G. Brown, M. Carlyle, J. Salmer´on, K. Wood, et al., "Defending critical infrastructure," Interfaces, vol. 36, no. 6, pp. 530–544, 2006.

[3] J. Arquilla and D. Ronfeldt, "Cyberwar is coming!," Comparative Strategy, vol. 12, no. 2, pp. 141–165, 1993.

[4] R. Clarke and R. Knake, Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins, 2010.

[5] C. Clausewitz, M. Howard, and P. Paret, On war. Princeton University Press, Princeton, NJ, 1976.

[6] P. Finn, "Cyber assaults on Estonia typify a new battle tactic," Washington Post, vol. 19, 2007.

[7] M. Lesk, "The new front line: Estonia under cyberassault," Security & Privacy, IEEE, vol. 5, no. 4, pp. 76–79, 2007.

[8] "Russian Invasion of Georgia. Russian Cyberwar on Georgia. Report of the Government of Georgia." http://georgiaupdate.gov.ge/doc/10006922/CYBERWAR-

[9] N. Falliere, L. O. Murchu, and E. Chien, "W32.Stuxnet Dossier," tech. rep., Symantic Security Response, October 2010.

[10] M. ENDSLEY, "Toward a Theory of Situation Awareness in Dynamic Systems," HUMAN FACTORS, vol. 37, no. 1, pp. 32–64, 1995.

[11] N. Castellan, Individual and group decision making: current issues. Lawrence Erlbaum, 1993.

[12] "CyberWar! Frontline - Intervies with John Arquilla." http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html/.

[13] K. Hwang, S. Kulkareni, and Y. Hu, "Cloud security with virtualized defense and reputation-based trust mangement," Dependable, Autonomic and Secure Computing, 2009. DASC '09. Eighth IEEE International Conference on, pp. 717 – 722, Dec 2009.

[14] "European Network and Information Security Agency." http://www.enisa.europa.eu/.

[15] NATO, "Concept for a NATO Security Management Infrastructure (SMI)," AC/322-D(2008)0049 (INV), Dec 2008.

[16] "ReMIND – Real-Time Machine Learning Intrusion Detection." http://www.first.fraunhofer.de/owx 1 4079 2 2 0 4be4ae1a1c59c1.html.

[17] O. K.-P. Karsten Bsufka and S. Albayrak, “Intelligent Network-Based Early Warning Systems.” http://dx.doi.org/10.1007/11962977, 2006.

[18] “Early Warning and Intrusion Detection based on Combined AI Methods." http://www.fides-security.org/.

[19] “Event Monitoring Enabling Responses to Anomalous Live Disturbances.” http://www.sdl.sri.com/projects/emerald/project.html.

[20] “Arakis dashboard.” http://www.arakis.pl/en/index.html.

[21] “CERT Polska.” www.cert.pl.

[22] “Worldwide Observatory of Malicious Behaviors and Attack Threats.” http://wombat-project.eu/.

[23] A. Shimoda and S. Goto, “Virtual Dark IP for Internet Threat Detection,” in APAN Network Research Workshop, pp. 17–23, 2007.

[24] S. Dharmapurikar, P. Krishnamurthy, T. Sproull, and J. Lockwood, “Deep packet inspection using parallel bloom filters,” in High Performance Interconnects, 2003. Proceedings. 11th Symposium on, pp. 44–51, IEEE, 2003.

[25] “sFlow.” http://www.ams-ix.net/technical/sflow.html.

[26] A. Serjantov and P. Sewell, “Passive-attack analysis for connectionbased anonymity systems,” International Journal of Information Security, vol. 4, no. 3, pp. 172–180, 2005.

[27] K. Wang and S. Stolfo, “Anomalous payload-based network intrusion detection,” in Recent Advances in Intrusion Detection, pp. 203–222, Springer, 2004.

[28] B. Swartout, R. Patil, K. Knight, and T. Russ, “Toward distributed use of large-scale ontologies,” in Proc. of the Tenth Workshop on Knowledge Acquisition for Knowledge-Based Systems, 1996.

[29] C. Index, “Global Mobile Data Traffic Forecast Update,” Cisco White Paper[Online]. Available: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.pdf.

[30] C. Index, “Global Mobile Data Traffic Forecast Update, 2009-2014,” White Paper, CISCO Systems Inc, vol. 9, 2010.

[31] P. Laud, “Handling encryption in an analysis for secure information flow,” in Proceedings of the 12th European conference on Programming, pp. 159–173, Springer-Verlag, 2003.

[32] C. Phua, V. Lee, K. Smith, and R. Gayler, “A comprehensive survey of data mining-based fraud detection research,” Arxiv preprint arXiv:1009.6119, 2010.

[33] S. Shahrestani, “Employing artificial immunology and approximate reasoning models for enhanced network intrusion detection,” WSEAS Transactions on Information Science and Applications, vol. 6, no. 2, pp. 190–200, 2009.

[34] F. Mattern and C. Fl¨orkemeier, “Vom internet der computer zum internet der dinge,” Informatik-Spektrum, vol. 33, no. 2, pp. 107–121, 2010.

[35] A. Farooqi and F. Khan, “Intrusion detection systems for wireless sensor networks: A survey,” Communication and Networking, pp. 234–241, 2009.

[36] F. Bustamante and D. Choffnes, “NEWS plugin for the Vuze (formerly Azureus) BitTorrent Client.” http://www.aqualab.cs.northwestern.edu/projects/NEWS.html.

[37] “Internet storm center.” isc.sans.org.

[38] “Active Threat Level Analysis System.” http://atlas.arbor.net/.

[39] T. Guo, “Shaping Preventive Policy in “Cyber War” and Cyber Security: A Pragmatic Approach,” 2011.