Cyber Security Policy. A methodology for Determining a National Cyber-Security Alert Level

Dan Constantin TOFAN[1], Maria Lavinia ANDREI[2], Lavinia Mihaela DINCĂ[1]
[1]Academy of Economic Studies, Bucharest, Romania
[2]Bucharest University, Bucharest, Romania
tofandan@yahoo.com, lavi_andrei@yahoo.com, lavinia.dinca@gmail.com

Nowadays, assuring the security of the national cyber-space has become a big issue that can only be tackled through collaborative approaches. Threats cannot be confined to a single computer system just as much as computer systems are rendered useless without being connected to a supporting network. The authors of this article propose an innovative architecture of a system designated to help governments collect and analyze data about cyber-security incidents, from different organizations, dispersed nationwide, and acting within various economic sectors. The collected data will make us able to determine a national cyber-security alert score that could help policy makers in establishing the best strategies for protecting the national cyber-space.

Keywords: *Cyber-Security, Incidents, Early-Warning, Intrusion, Detection*

1 Introduction

A big part of the daily human activity has been transferred in the online environment, and along with that so has the cyber-crime. Cyber-attacks are becoming more and more numerous and complex. There are countries that are developing real cyber-armies, ready to attack in no time.

Managing the security of an information system is not an easy job. We live in the XXI century that seems to be under the sign of major cyber-attacks and even under the sign of cyber-wars.

The Internet has become an international critical infrastructure and disturbing its functioning could cause big damages to any state. A good example in this area is the attack against Estonia in 2007. The country was literally wiped-out from the Internet because of a massive cyber-attack that succeeded in affecting numerous governmental websites and some financial institutions also. The attack lasted for 2 weeks.

The countries that have critical infrastructures based upon complex informatics systems, connected via the Internet (like the USA), are the first, and most vulnerable, that might suffer from such an attack. Usually, these countries are the most willing to invest in IT security.

William J. Lynn, United States Deputy Secretary of Defense stated in 2011 that USA could respond to cyber-threats with proportional military forces. He also stated that the cyberspace has become a new field of battle among land, sea and air [1]. The 2010 US Cyber Security Strategy also states that the cyber-security is one of the biggest challenges of the nation, because the Internet is one of the key factors related to economic competiveness and an indispensable instrument of the business environment. The digital infrastructure is considered a national asset, and protecting this asset is a national priority. [2]

Thus, we are assisting to a substantial transformation of the international cyber-space, as it becomes a key component of the world economy. Nowadays IT security has a new meaning: it is not a mere defensive concern, but it can also work as an offensive strategy.

The problem is that the state of security, be it about an organization or a state, becomes ever more difficult to accomplish through isolated or individual action. Securing and responding to threats by common efforts and cooperation of all parties that could be affected in case of a cyber-security incident, is now the new way of action in cyber-defence. This trend substantially mirrors the hacker community action, which now works at an international level, under the umbrella of or-

ganized-crime. When taking an organization, for example, either public or private, the cyber security issue cannot be tackled individually, but it will have to fulfill at least three conditions: (1) cyber-security legislation that will incriminate the cyber-attacks will have to be put in place, (2) proper actions will have to be taken by the authorities in charge of cyber law enforcement, (3) it needs the help of private security providers that will develop solutions to stop or mitigate the attacks. Security can no longer be locally addressed just by merely installing an antivirus or a firewall. Security must be addressed globally, beyond the borders of the physical network or the intranet. [3]

All in all, reaching the optimal level of security in the modern approach to cyber-security cannot be made individually, but with the involvement of all affected and responsible parties.

2 The concept of a National Early Warning System

The main idea brought forward in this article is that the efficient management of information security shifted from the individual approach, from the intra-organizational level, to a more cooperative approach involving as many of the concerned parties as possible [4].

The starting point in adopting this systemic approach of security will be the build-up of an Early Warning System (EWS) at national level. In this article we propose the architecture of a National Early Warning System, which will help in the determination of a national cyber security alert indicator, based upon the identification and analysis of a considerable number of cyber-security incidents collected from organizations all over the country. The national indicator will help in choosing the right policy decisions regarding cyber security strategies or attack mitigation measures.

The operating principle behind the EWS is represented by the real time collecting of data related to different cyber-security incidents, from computer systems operated by various organizations. In order to be representative at the national level, the EWS must collect incidents from a wide range of organizations, both public and private, of different sizes, within different economic sectors and homogeneously distributed across the country. Based on the network analysis of inputs about cyber incidents, identified within the partner organizations, the nature, distribution and intensity of those incidents could be determined. This is a very powerful feature that could be used for stopping a major incident to propagate to multiple systems. For example, if a bank is affected by a specific malware infection, and the incident is detected before spreading onto other banks, an alert is then sent out to all other potential victims ending up in reducing to minimum the distribution and the effects of the incident. Based on this early detection, the countermeasures could be rapidly developed, with the help of the community, and sent out to all interested or possibly affected parties.

As any alert system, so as to function properly, the EWS needs a series of important preconditions. As we have said before, an important condition for the well functioning of such a system is that information regarding cyber security incidents is collected from a very wide range of organizations and from multiple areas of activity. In this manner, we could observe if an attack is targeted at a specific field of activity (e.g. banks) or a specific geographical region.

Another important condition is that the participating organizations should be either usual targets of cyber-attacks or should be processing large amounts of traffic (ISP, Banks, Universities, Public institutions etc.). Of equal importance is that the data should be collected in real time, so that the alert and the reaction to it should be launched soon after the detection, and not after the attack has stopped and the damages have settled in.

Besides the conditions described above, an EWS should also accomplish some other requirements, such as:

- **Powerful correlation and aggregation algorithms:** the main purpose is that of correlating the data from different sources, so the existence of such algo-

rithms is a must.

- **Multiple methods of data collecting, regarding incidents**: the detection of malicious activities at network level is often done by classical IDS/IPS systems. A national EWS should use multiple methods for data collecting, not just IDS. An example should be log collecting, honeypots, netflow analysis, and anomaly detection.
- **Capacity of analysis of large amounts of data**: taking into consideration the complexity and dimension of the system, it will probably produce huge amounts of data that will need extensive processing capacity. Without such capabilities the system will collapse.
- **Scalability and platform independence**: these two characteristics are essential for detecting attacks within large-scale networks. Moreover, the technology used for intrusion detection must work independently of the type of equipment used by the organization that is hosting the sensor. (e.g. syslog capable).
- **Ability to capture data from mobile devices**: the mobile devices are continuing to grow in terms of proportions, and collecting data from this type of hardware is a real issue when developing such a system
- **Compatible with virtualized environments and cloud type services**: cloud computing and virtualization are the trends now when we speak about IT services, and such a system should not leave these technologies aside.

Implementing an alert system could prove of great help in detecting a large amount of cyber-attacks, such as: DDoS, SQL Injection, XSS, viruses, worms, Trojans, botnets. Nevertheless, these incidents could also be detected simply by implementing some IDS/IPS solutions in the organizations. The major advantage of such a system is that data is collected from multiple organizations and when aggregated and correlated at a central level, we can determine major security incidents that are targeted to specific types of organizations.

3 Who could build such a system?

Developing such a system is not an easy task. It has to rest on a set of varied types of organizations, public and private, acting in different sectors. Reason enough for the existence of a national authority, responsible for the Romanian cyber-space, is a must in building this system. Generally speaking, a strategy at national level cannot be fulfilled without the intervention of the state. That's why an authority responsible with building a EWS is the ideal option in this case. Moreover, the information gathered and analyzed by the EWS has policy implications and utility, and virtually no commercial use.

Among all Romanian authorities that deal with cyber-crime or are responsible with the security of the national cyber-space, we find one institution that better suits this role. CERT-RO is the National Computer Emergency Response Team, and among its responsibilities we can find:

- collecting and management of threats, vulnerabilities and cyber-security incidents, that are identified or reported to affect the Romanian cyber-space;
- national point of contact with other national or international CERT entities;
- provides assistance for national authorities in establishing cyber-security policies;
- provides assistance for organizations that operate or own critical infrastructures, regarding their cyber-security policies;
- develops or improves national regulations regarding cyber-security policies;
- real time warnings and reports related to nature and distribution of cyber-security incidents.

The importance of this structure is also stated in the National Security Strategy [5] and in the project of the national Cyber-Security Strategy [6].

Although the Government Decision no. 494/2011 establishing the role of CERT-RO, looks quite comprehensive at a first sight, the actual set up is rather unclear. The lawmakers did give CERT-RO some important roles, but they failed to specify how things must be done. If we take, for example, the real time

warnings regarding the nature and distributions of cyber-security incidents and national management of security incidents, they cannot be realized without the existence of a large amount of information related to different types of incidents. This type of data could be collected through a system like our EWS.
Participating in the EWS should not be mandatory. The system must prove its efficiency, and based on its gained reputation, it should attract different types of organizations. Nevertheless, the system must start with a minimum number of organizations, and therefore, a good strategy could be the involvement of public institutions. The cooperation between public authorities should theoretically be easier, and CERT-RO could work as the central point of such cooperation. Protocols with private companies have always been difficult, not only in Romania but in other countries as well, but they could eventually team up in a functioning system, given that its reputation is carefully safeguarded.

4 National Early Warning System Architecture

As mentioned before, the national EWS (NEWS) is a complex system that will connect different types of organizations, through a series of sensors installed in their computer systems that will ultimately be capable to detect many types of intrusions within the network.
Based on that information, aggregated and correlated within a central module, we could determine the nature, intensity and distribution of major cyber-security incidents that affect the organizations that installed sensors within their computer networks, even from the early stages of the attack.
We should mention that the system was developed to detect all kinds of intrusions, but the small ones will only be treated at local level, meaning that they will not be sent to the central database but will remain in the local one and will be treated by the local administrator or security responsible.
The proposed architecture of the national EWS consists of its components and a description of its underlying algorithm, used in determining the national cyber-security alert level.
Thus the national EWS is a composite system that uses multiple technologies and consists of the following three modules:

1. Event collecting module (MCE)
2. Alerting and Correlating Module (MCA)
3. Reporting module

The three modules design is represented in fig. 1. Following that, in the next subchapters we will present a functional and technical description.

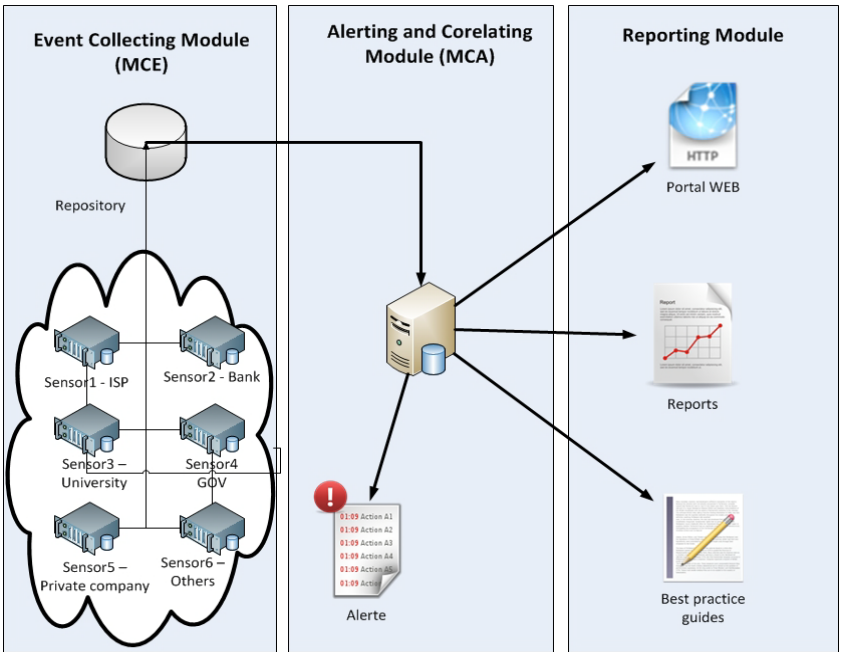

Fig. 1. NEWS Architecture

4.1. Event collecting module (MCE)

The role of this module is to analyze traffic data at the organizational level (local level) and to identify intrusions or potential incidents that could affect the organization's security level. The alerts resulted from the data analysis is sent to the central database (the next module) where the correlation process takes place. The traffic analysis is carried out through a sensor, which should be a distinct component installed inside the computer network. The sensor, a passive element of the network, will run an IDS/IPS service which will be able to analyze all the traffic processed by the system through the following technologies:

- traffic analysis through deep packet inspection;
- netflow analysis (source and destination IP addresses, source and destination ports, protocol used).

The traffic analysis will be carried out through the deep packet inspection (DPI) method, meaning that every data packet will be completely analyzed by an IDS/IPS application, which will determine the attack type based on comparing the packet with the signature from its database.

The DPI method is very efficient when it comes to detection or prevention of cyber-attacks or cyber-threats, because, unlike classic firewalls, the content of the packet is also analyzed along with the IP/TCP/UDP header. This allows the detection of a much wider range of attacks like viruses, Trojans, DDoS, or intrusions that manifest themselves through disturbances of the normal operating mode of a protocol. The IDS/IPS sensor is based upon the existence of some rules, also called signatures. If one of the rules is broken by the packet, or by a sequence of packets, the sensor will consider those packets as malicious and it will alert the security personnel and even prevent the packets from reaching their destination.

Netflow analysis is another type of traffic analysis used by our considered sensor. Netflow is a network protocol developed by CISCO for collecting data referred to source and destination addresses. A netflow record will contain data about source and destination IP addresses, source and destination ports and the protocol used for communication. These data are used for gathering statistics regarding network traffic, and could be used to determine some types of attacks such as flooding (DDoS).

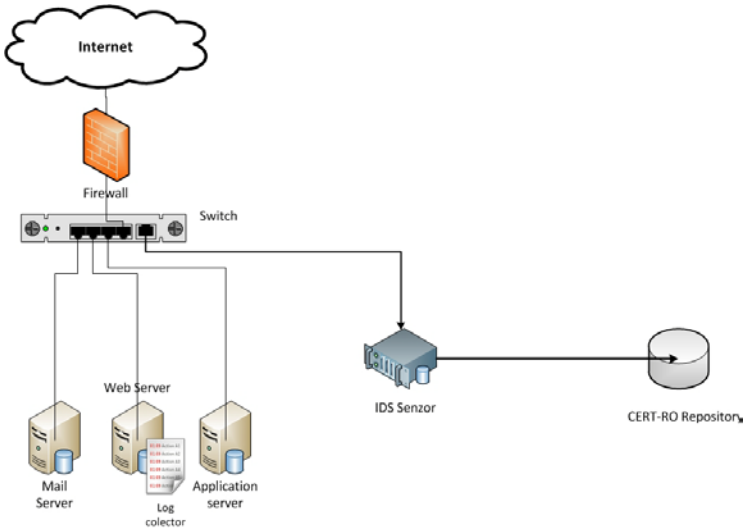

Fig. 2. Sensor within a network

Basically this module analyses the data traffic at the organizational level, and issues alerts about anomalies or intrusions detected inside the network. The alerts are transmitted to the central module of the national EWS, for aggregation and correlation with data

from other sensors. Fig.2 is a graphical representation on how MCE works.

4.2. Correlating and analysis module and the method for determining the national cyber-alert level indicator (MCA)

The MCA is the central module of the system. It is the module where all the data are collected and analyzed. It is the module that should, in our vision, be managed totally by CERT-RO, the authority that we consider to be most suitable for this job.

The purpose of the module is collection, aggregation and analysis of the data collected from the sensors spread at national level. By analyzing the correlated data, the system will be able to detect large or major cyber-attacks targeted to certain fields of activity (energy, transports, banks etc.) or groups of organizations.

The national EWS has a broader scope than just protecting the individual organization. It can determine the large scale attacks and mitigate them from early stages so that the damages would not be consistent. Depending on the type of attack, it could detect the pattern from the scanning stage, before the real attack has started. Correlation is the key element of the process, and is also the component that distinguishes a national EWS from simple EWS or other individual IDS/IPS solutions. The alert launched by the system will contribute to stopping the attack while the likelihood and impact of the threat is reduced consistently, and the attack could be stopped before gaining momentum. An attack that exploits specific vulnerabilities will trigger security alerts to other organizations affected by that vulnerability in order to prevent the attack from spreading. Therefore, the MCA module is a key component in this distributed cyber-security system.

This module has also a public policy role: that of determining a national cyber-security alert indicator. Based on the analysis of the information that it collects, the module calculates an indicator through analyzing the entire dataset, an indicator that will measure the general level of threat in terms of cyber security. This indicator will be an important tool for the policy makers in the area of protection and regulation of the cyber space. We have argued before that the cyber space is increasingly important in terms of social life and economic activity. It therefore cannot leave aside the political arena either. Policy is growingly concerned with cyber security, and large cyber-attacks are, naturally, in the attention of the policymakers.

The fact that the system collects data from multiple organizations, from different geographical areas and different fields of activity, makes it representative countrywide or at certain levels of the economy. The main idea is to top the proportionality of such a model with the aforementioned national security policy role, thus gaining an effective methodology for measuring a cyber-alert security indicator based on which the real level of security within the country could be determined. With this indicator in view, policymakers could take decisions to tackle cyber problems or, on the contrary, to ignore false alarms.

The key factor when determining this indicator resides in correlating the profile of the organization with the profile of the cyber-security threat. Correlation of these variables would result in a realistic score of the incident. Based on incident score, future calculations must be done in order to obtain the national indicator.

Let’s then consider how these profiles should look like. In Table 1 we will define the profile of the organization, and in Table 2 we will define the profile of the threat.

Table 1. Profile of the organization

No.	Variable	Explanation
1	Field of activity	This variable is used for classifying the cyber-attacks with regard to the economic sector that they target. In this manner, the indicator could also be determined per field of activity, and the organizations within that filed could have a more accurate view of their vulnerability to cyber crime. We have considered the following 12 main domains of activity included in the proposed national EWS: • Public administration • Public / National safety and public safety • Public / E-government services • Agriculture / Food Related Services • Auto / Transportation • Banks / Insurances / Finances • Education / Culture / R&D • Energy / Petrol / Chemistry • Health / Medicine • Software / IT Services • Telecom / Internet • Others
2	Organization type	Public, private or NGO. Although rather simplistic, as we see nowadays complex organizational setups (e.g. Quangos, PPPs, multinational organizations, etc), this variable continues to be relevant. The three main categories of organizations have distinctive behaviours in terms of tackling their cyber vulnerabilities and cannot be ignored by our indicator.
3	Organizational level of security	This level is defined on a scale of 1 to 5, where 5 is considered the most secured level. The position on the scale is determined by the sensor installation using a scale inspired from the ISO 27001 standard, as follows: 5 – functional firewall, IDS/IPS, anti-malware solution, up to date systems, vulnerability scanners, email filtering, VPN for extranet; 4 – functional firewall, anti-malware solution, up to date systems, email filtering, VPN for extranet; 3 - anti-malware solution, up to date systems, email filtering; 2 – not fully functional firewall, not up to date anti-malware solution; 1 – no firewall, no antimalware, obsolete operating systems.
4	Critical infrastructure or not	The system must also be able to distinguish between critical infrastructure systems and non-critical infrastructure systems. It is an important classification because critical infrastructures are the heart of every national security system.
5	Importance of confidentiality of information	On a scale of 1 to 5, 5 being the most important, we will determine the importance of data confidentiality within the participating organizations. The value of 5 is only awarded to critical infrastructures. (5 – very big, 4 – big, 3 – medium, 2 – low, 1 – very low)
6	Importance of availability of information	On a scale of 1 to 5, 5 being the most important, we will determine the importance of data availability within the participating organizations. The value of 5 is only awarded to critical infrastructures. (5 – very big, 4 – big, 3 – medium, 2 – low, 1 – very low)

7	Importance of integrity of information	On a scale of 1 to 5, 5 being the most important, we will determine the importance of data integrity within the participating organizations. The value of 5 is only awarded to critical infrastructures. (5 – very big, 4 – big, 3 – medium, 2 – low, 1 – very low)

The organizational profile will be considered when determining the real impact of a threat to the organization's computer system and to their assets. Nevertheless, so as to determine the real severity of a cyber-security incident, a series of variables must be defined for the operationalization of the threat itself. It is quite possible that threats targeting an organization, will not affect the computer system, because of particular characteristics, for instance the absence of the specific vulnerability that could be exploited. The attack could also be targeted to unimportant or redundant computer systems, without real worth for the organization. In this case the incident should not raise artificially the level of the score, because otherwise the indicator will lose in terms of accuracy. Consequently, a profile of the attack must also be defined. In the table below we exemplify a method for measuring such a profile.

Table 2. Incident profile

No.	Variable	Explanation
1	Attack category	The list of attack types could look like this, although some other types of attacks could be added: 1. DDoS / DoS 2. Code Injection (SQL etc.) 3. Malware 4. Botnet 5. Phishing 6. Spam
2	Level of threat	The level of threat is defined on a scale of 1 to 5, 5 being the most dangerous incident. This variable defines the external conditions of an attack, and takes in consideration independent variables that could affect the result of an attack. 5 – there are specific vulnerabilities that can be exploited, and will grant the attacker administrator privileges upon the targeted system. 4 - there are specific vulnerabilities that can be exploited, and will grant the attacker user level privileges upon the targeted system. 3 – there are no specific vulnerabilities that can be exploited by the threat, but the attacker could gain administrator privileges upon the targeted system. 2 - there are no specific vulnerabilities that can be exploited by the threat, but the attacker could gain user level privileges upon the targeted system. 1 - there are no specific vulnerabilities that can be exploited by the threat, and the attacker cannot gain user level privileges upon the targeted system.
3	Level of severity	It is defined on a scale of 1 to 5, 5 being the most severe incident. The variable defines what type of equipment is targeted by a threat, and could have the following values: 5 – critical equipment that assure the well-functioning or security of the network (router, firewall etc.); 4 – critical application servers (web, mail, etc.);

		3 – other servers, applications or hardware which ensure the well-functioning of the computer system; 2 – final user PC's or laptops, that are part of a network; 1 – home users.
4	Confidentiality	This variable should have positive values if the attack is likely to affect confidentiality of information.
5	Integrity	This variable should have positive values if the attack is likely to affect integrity of information.
6	Availability	This variable should have positive values if the attack is likely to affect availability of information.

Establishing a link between the threat and the target itself is an essential process of the national EWS. The alerts or the indicator itself can be influenced by miscalculation of the incident score, or the miscorrelation between the attack and the organization.

In other words, considering an attack that triggers losses in terms of confidentiality of information, which will target an organization that does not consider confidentiality to be crucial for the organization; it will not impact too much the national indicator as the incident score will be rated low.

For the calculation of the incident score, a well-structured algorithm must be defined. Hence, the incident score will be determined after the correlation of the organization profile and incident profile. Here is what has been considered as ideal for determining the incident score. Let us look into the following formula:

Incident score = (Organization's level of security + CIA importance) – (Level of danger + Level of severity)

Where:

CIA importance = the actual impact of the threat upon the organization in terms of the effect of the incident upon the overall quality of the information (confidentiality, integrity, availability). Actually, we will multiply the value defined as "importance of confidentiality for an organization" with 1, if the threat affects confidentiality, or with 0, if it has no impact upon the confidentiality. The same pattern is applied to integrity and availability of the information. In the end, we compose an average of the 3 values and obtain the "CIA importance" score.

Given that the score can vary quite a lot, and the scale proposed for measuring the national alert indicator is 1 to 5, the score of the incident must be brought down to the same scale. Thus, when defining the ***incident level of alert,*** we would use the scale presented in Table 3, which will also be considered later on when determining the national indicator.

As an example let us consider a public organization with the level of security scaling 3 (anti-malware solution, up to date systems, email filtering). Let's assume they do not manage any critical systems and have considered the importance of information properties as follows: confidentiality – 5, integrity – 5, availability – 3. This organization would, in our example, be confronted with an SQL Injection attack that is generally considered a threatening attack, scaling 5, and with a rather high level of severity, scaling 4. This kind of attack has consequences upon the integrity and the availability of the target information or computer system. When taking into consideration the organizational profile and the threat profile, we should refer to the formula above, inserting the values mentioned above.

Incident score = (3+(5x1+3x1+5x0)/3) - (5+4) =5,3 – 9 = -3,6

Continuing our example, when comparing the resulting scores with those from the table below, we can determine that the in-

cident level of alert is HIGH, meaning that the organization is in real danger, and the attack could lead to serious damages.

Table 3. Incident's level of alert

Incident level of alert	Value obtained
CRITICAL (5)	< -4
HIGH (4)	from -4 to -2
MEDIUM (3)	from -1,99 to +2
NORMAL (2)	from +2,01 to +5
LOW (1)	> +5

Based on the incident score, we would be able to determine the national indicator. However, some prior steps need to be taken: The first step is to (1) calculate given a certain time interval, a set of two indicators for each field of activity, one for critical infrastructures, and one for non-critical infrastructures. The indicators would thus be determined as an average value of the registered incident scores, in that given time frame. One of the indicators is for the critical infrastructures and one for the non-critical infrastructures. Below is the mathematical representation of the two indicators:

$$S_C = \frac{\sum_{j=1}^{nr} S_{j_C}}{nr}$$

$$S_{non} = \frac{\sum_{j=1}^{nr} S_{j_{non}}}{nr}$$

where:

S_C = critical score - average of the values recorded as final scores of the incidents that affected critical organizations within a certain area of activity (e.g. Education / Culture / R&D), in a given time interval. The score is considered critical because it refers to organizations that manage critical infrastructures.

S_{non} = non-critical score – average of the values recorded as final scores of the incidents that affected non-critical organizations within a certain area of activity (e.g. Education / Culture / R&D), in a given time interval. The score is considered non-critical because it refers to organizations that do not manage critical infrastructures.

nr = number of incidents that affected organizations from an area of activity, in the given time frame.

S_{jC} = the score of one cyber-incident, that affected one organization, from a certain area of activity (e.g. Education / Culture / R&D), that manage critical infrastructure systems.

S_{jnon} = the score of one cyber-incident, that affected one organization, from a certain area of activity (e.g. Education / Culture / R&D), that doesn't manage critical infrastructure systems.

We should mention that specific areas of activity that do not record cyber-security incidents will be scored 1, meaning the lowest level of alert. Applying the formulas described above we then pass on to determining the overall score of the area of activity. We would be using the scores for the critical organization and the scores for the non-critical organization, weighted by the percentage they represent within the total, for each area of activity, using the following formula:

$$S_d = a_i * S_{i_C} + b_i * S_{i_{non}}$$

where:

S_d = the score for one area within a certain timeframe.

a_i = the percentage of organizations within a certain field that have critical infrastructure systems.

b_i = the percentage of organizations within a certain field that do not have critical infrastructure systems.

After obtaining an average score for every field, we must determine a national indicator for all the organizations included in the national EWS. Following the previous formulas, the national indicator would look like this:

$$I_{NAT} = \sum_{i=1}^{n} x_i * S_{i_d} = \sum_{i=1}^{n} x_i * (a_i * S_{i_C} + b_i * S_{i_{non}})$$

where:
I_{NAT}= National Cyber-Security Alert Indicator.
x_i = the percentage of organizations within a certain field of activity out of the total number of participating organizations.
S_{id} = the score for a certain field of activity, in a given timeframe.
n = the total number of economic sectors (12).
Based on the methodology described above, the national indicator could have values between 1 and 5, 5 being the worst state of security, and 1, the best. In Table 4 below we can find a description of these values.

Table 4. Values taken by the national indicator

CRITICAL	Correlated cyber-security incidents, intentionally launched, that have strategic targets, and could affect the security of the national cyber-space and could cause big damages to the national economy.
HIGH	Correlated cyber-security incidents, intentionally launched, that have strategic targets, and could affect a certain economic sector or a certain type of organization, without causing big damages to the national cyber-space or to the national economy.
MEDIUM	Correlated cyber-security incidents that could affect various organizations without causing big damages to the national cyber-space or to the national economy.
NORMAL	Isolated incidents, that affects various types of organizations, without causing big damages to the national cyber-space or to the national economy.
LOW	Isolated events, of low severity, affecting various organizations nationwide.

The indicator could be measured at various time intervals (monthly, yearly or even daily). From the above formula we could also derive the indicator for the critical infrastructures or for the non-critical infrastructures. It is convenient to do so because, in case of big values of the indicator, the counter-measures should first be taken for critical systems.
We have thus described the methodology used for obtaining a national cyber-security alert indicator. This indicator is prone to reflect the actual situation regarding the nationwide level of cyber-security, extrapolating from the registered security incidents affecting the participating organizations.
Unfortunately an exemplification of the way the indicator works on real data exceeds the aims of the present article, for a few reasons other than the obvious space requirements. First of all, at this moment, there is no such data collected nationwide. Although CERT-RO was set up in July 2011, in the short time passed, they could not build up a significant database. CERT-RO has gathered now data on less than 100 incidents. Moreover, a big part of the data has been collected only from public or governmental institutions, failing to access information from private actors. The calculus will be of real use only after the alert system is set up to include a representative sample of organizations.

4.3. Alerting and reporting module (MAA)

The alerting module of the national EWS is also very important because it represents the basis for the action to be taken in case of major security incidents. Practically speaking, when a major attack is detected, meaning an attack that affects several organizations and that follows certain patterns (e.g. the same IP source is identified to attack multiple organizations), we could conclude that the attack is intentionally launched and could affect more targets in the near future. At this stage, alerts would be sent to all possible victims, warning them about the imminence of the attack. Such a policy would increase the chances that an organization would adopt the necessary measures to mitigate the negative effects. [7]
The national EWS would generate a consistent database registering all the threats that affected the participating organizations. Through the MCE module the information would be collected at the central level and through the MCA module, important correlation and aggregation algorithms are applied

to the collected information. In this way major cyber security incidents would be detected. Therefore, the central level of the system (CERT-RO) would hold a huge amount of information that could represent solid evidence in support of decisions taken by policy makers in the field of cyber-security. The national cyber-security strategy could be grounded in the information provided by the national EWS. Adopting the optimal security measures or the regulations needed for cyber-crime mitigation should also be supported by relevant information collected at national level. Obviously, the national EWS would fulfill the above conditions.

In order to develop such a system, the initiator must have powerful reporting capabilities. Therefore we suggest that the system should also have some reporting capabilities that could have the following functionalities:

- web portal – the most common or dangerous threats, identified after the aggregation and correlation process, will be published on a web portal, open to the public. The scope is to increase the awareness of the possible targets or other security specialists, about the real dangers that could affect the national cyberspace.
- cyber-security reports – based on the collected information, the system would furnish statistics relevant for decision makers nationwide. Nowadays such statistics do not exist in Romania, so we believe that these kinds of reports will be much appreciated by both private and public organizations, along with authorities that deal with cyber-crime.
- best-practice guides – the most common attacks nationwide should have a special treatment, meaning that countermeasures or specific recovery strategies should be developed for the affected parties or possible targets.

5 Conclusions

This article points out that assuring cyber-security within an organization needs nowadays a more collaborative approach. Threats cannot be confined to a single computer system just as much as computer systems become useless when working in isolation. Interconnectivity forces organizations to better protect against cyber-crime, also contributing to the cyber-security community.

When speaking of national cyber-security there is no other way than cooperation between involved parties [8]. In this complex and risky cyber environment, policymakers need help in deciding what represents a threat and how to tackle it. Therefore, they need simple and reliable information, such as an indicator, that should help them understand the cyber-threats and define strategies for securing the national cyberspace against them.

The methodology and the system architecture proposed here are designated to help the governments collect and analyze data about cyber-security incidents, and determine a cyber-security alert level for their countries.

The article might seem rather prescriptive, in the sense that it tries to propose a real institutional setup and specific implementation strategies for the national EWS. Nevertheless, most of the proposals suggested here have been paid growing attention by the national security bodies worldwide, and Romania has to start thinking more thoroughly about its cyber status quo, as well.

References

[1] W. J. Lynn, *Deputy Secretary of Defence, Public speech as delivered at National Defence University,* Washington, D.C., July 14, 2011.

[2] The White House, *USA National Security Strategy,* May 2010, USA, [Online] Available at: www.whitehouse.gov

[3] M. Golling, B. Stelte, ”Requirements for a Future EWS – Cyber Defence in the Internet of the Future” *In 3rd International Conference on Cyber Conflict*, Tallinn, Estonia, 2011, pp. 1-16.

[4] P. Trimintzios, C. Hall, ”Resilience of the Internet Interconnection Ecosystem”, *European Network and Information Security Agency* [Online], 2011, Available at: http://www.enisa.europa.eu/activities/res/other-areas/inter-x/report/interx-report?searchterm=internet+resilience

[5] Romanian Presidency, *National Defence Strategy*, 2010, [Online], Available at: http://www.presidency.ro/static/ordine/SNAp/SNAp.pdf

[6] Ministry of Communication and Information Society, *Romania's national Cyber Security Strategy – Project*, 2011, [Online] Available at: http://www.mcsi.ro/Transparenta-decizionala/21/Strategie_Cyber_23052011

[7] U. Flegel, J. Hoffmann, M. Meier, "Co-operation Enablement for Centralistic Early Warning Systems", *Proceedings of the 2010 ACM Symposium on Applied Computing*, 2010, New York USA, pp. 2001-2008, ISBN: 978-1-60558-639-7.

[8] S. Kim, S. J. Shin, "Hybrid Intrusion Forecasting Framework for Early Warning System", *IEICE TRANSACTIONS on Information and Systems*, Vol. E91-D, No. 5, pp. 1234-1241, No.5, May 2008, pp. 1234-1241.

Dan TOFAN has graduated the Faculty of Computer Science for Business Management within the Romanian-American University in 2005. He holds a Master Degree in Computer Science obtained in 2007 from the Bucharest AES. He is a PhD candidate since 2006 at the Doctoral School from the Bucharest Academy of Economic Studies. His work focuses on the information security and study of major cyber-security incidents. He joined the CERT-RO team in May 2011 and he is now working with them in responding to cyber-security incidents that affect Romania's organizations.

Maria Lavinia ANDREI is a policy expert holding two master's degrees from King's College London, UK and the National School of Political Science and Administration, Bucharest, Romania. She has recently been granted the PhD title in Sociology at the Bucharest University with a thesis entitled "Evidence Based Policy. Bridging the gap between social science and public policy". She is also an expert in public programs' implementation and European Structural Funds projects management.

Lavinia Mihaela DINCA has graduated the Romanian American University and currently holds two master degrees in: "Business Excellence Models" from Academy of Economic Studies Bucharest and "Computer networks" from University of Bucharest. She is currently enrolled in the doctoral programme at the Academy of Economic Studies Bucharest. She has experience in managing software complex projects being PMP certified. Her main interests are: steganography, cryptography, computers security, Linux and open source software.