2014 6th International Conference on Cyber Conflict
P.Brangetto, M.Maybaum, J.Stinissen (Eds.)
2014 © NATO CCD COE Publications, Tallinn

Beyond technical data - a more comprehensive Situational Awareness fed by available Intelligence Information

Andreas Kornmaier
Faculty of Computer Science
Universität der Bundeswehr München
D-85577 Neubiberg, Germany
andreas.kornmaier@unibw.de

Fabrice Jaouën
Deputy Assistant Chief of Staff - CJ35
Multinational Joint Headquarters Ulm
D-89081 Ulm
fabricejaouen@bundeswehr.org

Abstract: Information on cyber incidents and threats are currently collected and processed with a strong technical focus.

Threat and vulnerability information alone are not a solid base for effective, affordable or actionable security advice for decision makers. They need more than a small technical cut of a bigger situational picture to combat and not only to mitigate the cyber threat.

We first give a short overview over the related work that can be found in the literature. We found that the approaches mostly analysed "what" has been done, instead of looking more generically beyond the technical aspects for the tactics, techniques and procedures to identify the "how" it was done, by whom and why.

We examine then, what information categories and data already exist to answer the question for an adversary's capabilities and objectives. As traditional intelligence tries to serve a better understanding of adversaries' capabilities, actions, and intent, the same is feasible in the cyber space with cyber intelligence. Thus, we identify information sources in the military and civil environment, before we propose to link that traditional information with the technical data for a better situational picture. We give examples of information that can be collected from traditional intelligence for correlation with technical data. Thus, the same intelligence operational picture for the cyber sphere could be developed like the one that is traditionally fed from conventional intelligence disciplines. Finally we propose a way of including intelligence processing in cyber analysis.

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of any agency of the government. Examples within this article are based only on very limited and dated open source information. Assumptions made within the analysis are not reflective of the position of any government entity.

We finally outline requirements that are key for a successful exchange of information and intelligence between military/civil information providers.

Keywords: *cyber, intelligence, cyber intelligence, information collection fusion*

1. INTRODUCTION

Cyber attacks and incidents take place on a daily basis, but only few become known to a broader community. Nevertheless, the known cyber attacks with their severe results, e.g. the closure of the company HB Gary Federal, motivate IT Security to improve defensive measures to protect their organizational networks and the data and information stored in these.

In order to protect the networks they are monitored with sensors and tools on servers and network nodes to provide lower-level network event-oriented alerts. The use of the tools and the analysis of the lower-level data require in most cases highly technical trained network security experts.

They are also analysing detected attacks to understand how the attacker was able to gain access to the system using vulnerabilities and weaknesses in hard- and software and their configuration [1].

The information collected by the sensors and the evaluated attack data that are currently collected and processed have a strong technical focus that is mainly directed inwards.

Threat and vulnerability information alone are not a solid base for effective, affordable or actionable security advice for decision makers. They need more than a small technical cut of a bigger situational picture not only to mitigate, but to combat the cyber threat. The technical information needs to be transferred from "geek" vocabulary to a format understandable by the decision maker [2]. Nevertheless, one must admit that not even when this process is completed the decision maker has a real and full understanding over the situation, although this should ideally be appropriate for him to develop and coordinate detailed plans, ensuring by the way that he stays interested in cyber defence planning [2].

Thus, cyber specialists are encouraged to go this way as it is true that the principles of war have not changed with the development of the cyber dimension. Clausewitz' statement "War is the province of uncertainty: three-fourth of those things upon which action in war must be calculated, are hidden more or less in the clouds of great uncertainty."[3] applies to features of the modern Information Technologies. The tempo set by cyber-attacks, in some cases their hidden or at least discrete infiltration into the systems keep the decision maker in a false sense of security, being completely ignorant of the inherent danger. On the other hand, lacking any understanding in cyber matters could as well drive him to a form of paranoia by fear of full scale cyber-attacks, this feeling being fed by some part of irrationality.

In that sense the cyber specialist plays a critical role in the decision making process, helping the leader to strike a balance in the effective threat level posed by cyber issues. Fully involved in the leader's support and advisors' team, this expert is expected to cover one major task: developing the awareness on cyber issues in support of those making a decision.

Therefore it is necessary to transfer the technical information into the language of the decision maker and put it into his/her context by supplementing the technical monitoring data with

further available information or intelligence [4], thus relating the cyber dimension to the overall operational framework. This approach will also provide a more extensive situational awareness, enabling a more comprehensive decision making. The required information is very often already available, even correlated, but not linked. Thus, it is now necessary to take a look at already available conventional data that needs to be collected and fused with the traditional security event data, not only to be reactive to threats, but to be enabled to predict and prevent attacks [5].

Very little research has addressed the use of already available information to put technical data into an operational/ strategic context. In this paper, we first give a short overview over the related work that can be found in the literature. We then evaluate the approaches. Following this we examine what information categories and data already exist, identify information sources in the military and civil environment, before we propose to link that traditional information together with the technical data for a better situational picture. Finally we propose a way of including intelligence processing in cyber analysis.

This paper is not intended to describe specific techniques or potential theoretical frameworks for a better situational awareness through correlation of context information. Legal constraints and regulations like privacy laws that legitimately limit data acquisition are also beyond the scope of the effort of this paper. This is also the case for lack of cross-border treaties for data sharing and data constraints and restraints that might exist in regards to mission, civilians, enemy, time, ROE.

We further identify requirements, where information needs proactively to be looked for by tasking. We approached the field through a literature review, experience, participation in cyber defence exercises and many fruitful discussions with IT Security specialists and intelligence officers.

In the next section we begin by describing the related work identified by performing a literature review on conventional data and information to be used for better situational awareness and more comprehensive decision making in the cyber context complementing technical data.

2. RELATED WORK

For the literature query we were looking at several approaches in the literature for fusing data and structuring information in a format. We also looked at contributions to situational awareness, the common operational picture (COP) and the decision making during the literature review. All papers have a limited focus in regards to our research, so we only touch the most relevant developments with findings for our research.

In [6] we found generic threat matrixes that allow to categorize threats and thus to define a common vocabulary for them. Although a common terminology as a basis for successful understanding of different groups (e.g. technicians and decision makers) is still missing [2], some different categories of players can be discriminated [7]. While in the past and in some current conflicts the organized masses (states, armies, ethnicities) of people were at the core of the analysis, the cyber dimension has led to the emergence of smaller groups or even individuals as possible adversaries of a much larger organization.

Opposing in some way Clausewitz' approach of war to the cyber dimension of conflicts, Kempf

underlines the emerging role of the individual. While in former albeit various forms of conflicts between states, organized bodies were in the leading role, individuals are now able to operate, even in a limited dimension, against stronger, larger structures from remote and safe locations. In addition to those isolated persons, formal or informal groups act in the cyber dimension, either motivated by crime or political activism, finding there a good opportunity to set plans, reach their goals or get some financial or political profit.
However, their large diversity prevents the analysts from any simplification as this could drive them to a misleading understanding of the threat. As a matter of fact, the knowledge of the 'hostile' Tactics, Techniques and Procedures (TTP) has to be permanently checked and balanced with the effective capabilities of the most probable adversary, without excluding the other ones. Yet, this overall framework being in a permanent movement and transformation plays different roles in the decision making of leaders, depending on their objectives and on the vulnerabilities offered in reaching for their own goals to those individuals or groups.

The large amount of potential third players who could influence the own action gives then the analysis of the cyber threat a paramount importance, in order to provide the leader an appropriate level of information before making his decision.
To reach this goal a structured and comprehensive approach is required and provided by different tools developed by the specialists in cyber issues. If not, the result would be giving the potential threat an infinite complexity that would severely hamper any trial for a sound cyber defence.

The Structured Threat Information eXpression (STIX) is a collection that includes various sets of cyber threat information. The available sets in STIX offer a structure to store information on Indicators, Incidents and Adversary TTPs including attack patterns, malware, exploits, tools, infrastructure, targeting, etc. Also information on exploitable targets like their vulnerabilities and weaknesses can be put into STIX, as well as different remedial actions (Courses of Action) to respond to incidents or to vulnerabilities/weaknesses.
In STIX also information can be included on Cyber Threat Actors and their Cyber Attack Campaigns [1].
For the representation of the information STIX uses other, already developed structures. For information like 'cyber observables' (operational cyber events or stateful properties such as registry keys, email, and network flow data) it uses the definitions of the Cyber Observable eXpression (CybOX) language. The Common Vulnerability Enumeration (CVE), Common Platform Enumeration (CPE), Common Weaknesses Enumeration (CWE), and Malware Attribute Enumeration and Characterization (MAEC) are ingredients of STIX to describe standard information about vulnerability (using OVAL, the Open Vulnerability and Assessment Language), platform, weakness and malware. For describing an attack it uses the Common Attack Pattern Enumeration and Classification (CAPEC).
In summary it can be stated that STIX allows to represent cyber threat information in a structured, standardized manner [1].

Data fusion is in [8] described to be extended into the cyber security incident management domain. In [9] the basic data for several fusion levels come from Sys Logs, Web Logs, IDS and IPS alerts. All four data sources are technically aligned in that Data Fusion Approach for Cyber Situation Awareness and Impact Assessment.

Other approaches focus on establishing a methodology or metrics to characterize the threats consistently and add with the measured observables to a situational picture [4], [6].
Usually open-source information is utilized and not necessarily secret intelligence [4], although the latter will never be excluded depending of the threat level against the vital functions of the target.
Hutchins states in [10] that "it is possible to anticipate and mitigate future intrusions based on knowledge of the threat" and proposes an "intelligence-driven, threat-focused approach to study intrusions from the adversaries' perspective."
In the military and security environment the term intelligence stands for understanding and knowledge in the military and security context. But it is also used for reports and summaries that provide information with an assessment and added benefit to decision makers, operational planners and intelligence specialists to round up their situational picture for their further work [11], [12].
Classical questions for the intelligence community are the adversary's intent as well as TTPs.
In the context of countering Cyber Terrorism David proposes in [5] the establishment of a Cyber Intelligence Analysis Centre generically outlining a cooperation of governmental and civil entities focusing on technical means.
[5] postulates that intelligence "should provide the essential elements of enemy information: who, what, when, where, why and how. That is, who will attack what, at what time and place, for what purpose and objective, and with what type of resources and methods."
In [5] it is proposed to achieve this goal by fusing information from multiple sources to learn and analyse the tools, tactics and motives.

As traditional intelligence tries to serve a better understanding of adversaries' capabilities, actions, and intent, [1] argues that the same is feasible in the cyber space. He uses the term cyber intelligence for this cyber focused field. According to [1] cyber intelligence is to give responses to relevant threat actors, their suspected intent, and adversary's possible and taken Course of Action. This includes technical targets like sort of vulnerabilities, misconfigurations, or weaknesses an opponent is likely or used to exploit in attacking their objective [1]. To achieve this, cyber intelligence has to analyse opponent's capabilities in the form of their TTPs. TTPs are derived from the traditional military sphere, where they are used to analyse and predict an adversary's actions and methods. Therefore, TTPs have a central role not only in traditional intelligence, but also in the cyber sphere [1].
Nevertheless, all approaches are missing to take a view on already available information, traditional established information structures and how they could be benefited from.

3. EVALUATION OF EXISTING APPROACHES

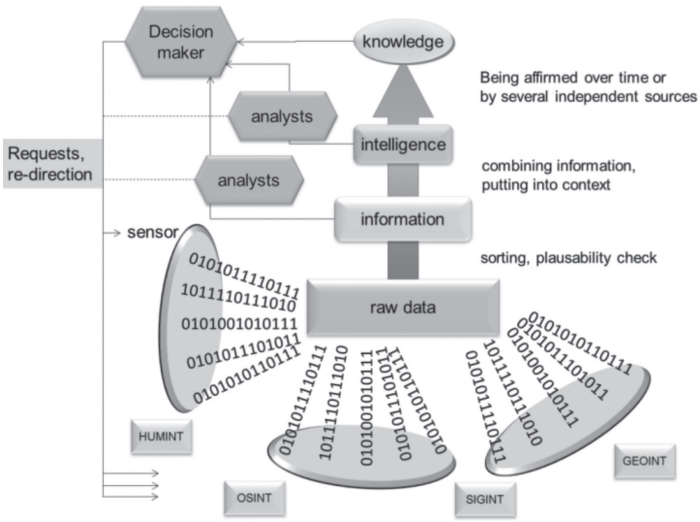
Our centre of interest being set on the efforts to collect, link and fuse information or exchange it [8], we left apart the understanding of the different groups, for which we suggest to refer to already existing typologies [6], [7].

In the related work the focus is mostly set on technical (network- and packet-level) data derived from lower-level security tools and their storing in data structures for further processing as

described in [1] and [9]. That information is of course relevant to describe a network topology or events within a known network infrastructure [13].
For this purpose STIX includes several other well defined and established structures. It can be summarized as overarching framework of several specialized smaller frameworks. Nevertheless, all found efforts concentrate on technical aspects and their assessment. But it must be stated, that threat and vulnerability feeds by themselves do not produce intelligence on cyber threats. Nor are the results effective or actionable in regards to a situational awareness or for a decision making.

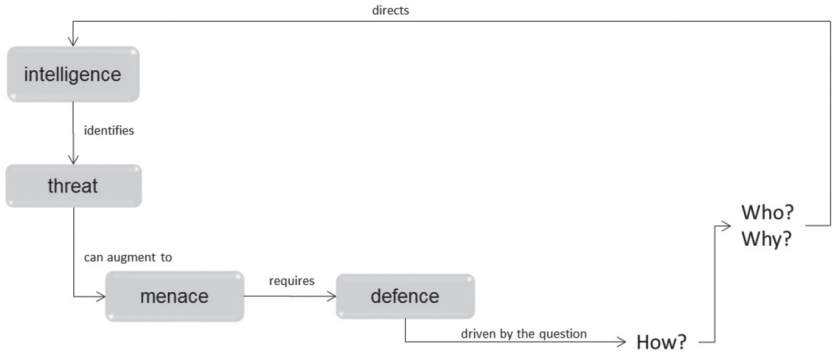
At first technical data comes unstructured and it needs to be decided, what is relevant and/ or representative for further processing and assessment by a skilled analyst [6], [14] (comp. figure 1).

FIGURE 1: PROCESSING OF RAW SENSOR DATA TO INTELLIGENCE AND TO KNOWLEDGE; READJUSTMENT OF SENSORS (OWN ILLUSTRATION)



He can assess the actual and mostly historic data to give an estimate on the current threat or on a preceded attack/incident from a technical perspective. That kind of information has been seen as an important type of knowledge by almost all above described approaches. But for a proper assessment on a more abstract layer, where non-technical information is in the focus, further information that is collected and processed is needed. For example in an assessment on taken informational damages during an incident/ attack that bases solely on technical data, it is mostly analysed “what” has been done, instead of looking more generically for the tactics, techniques and procedures to identify the “how” it was done [10]. The “how” allows the defender to evaluate capabilities and objectives, maybe even limitations and doctrine of the attacker [10] (comp. figure 2).

FIGURE 2: IMPORTANT ROLE OF INTELLIGENCE (OWN ILLUSTRATION)



In some way, critically needed are "intelligence-based earliest assessments of adversaries' intent" [4].

The intelligence analysis gets its real value by prioritizing the potential threats depending on their level of technological danger and their will or intent to effectively disturb the networks or activity of own assets. Dossé pledges for such a discrimination of the threat [15]; e.g. in conventional military assessment, the different levels of threats are to be discriminated: a single man attack with a rifle that is not considered to be at the same level as an offensive with an armoured corps.

Very often the statistics published by administrations do not help figuring out the effective threat they are confronted with, as they release the number of attacks they are confronted with on a certain period of time, without sorting out which were of critical importance and which could be simply disregarded as considered irrelevant.

Although it has never been and will never be an exact science, intelligence analysis provides the appropriate understanding needed to support a sound and efficient decision process.

The combination of capability and intent allows an assessment beyond forensic after-attack assessments in form of predictions and warnings that address events in the (near) future [4].

The approaches that are based on technical data miss mostly the aspect of the adversary's intent, also if expressions like adversary's intent, Tactics, Techniques, and Procedures, courses of action are considered, but they are used always in a technical context. Also if technical experts hypothesize about intent and goal of attacks, the "task of drawing such conclusions is more professionally handled by judiciary, intelligence and diplomatic authorities" [8].

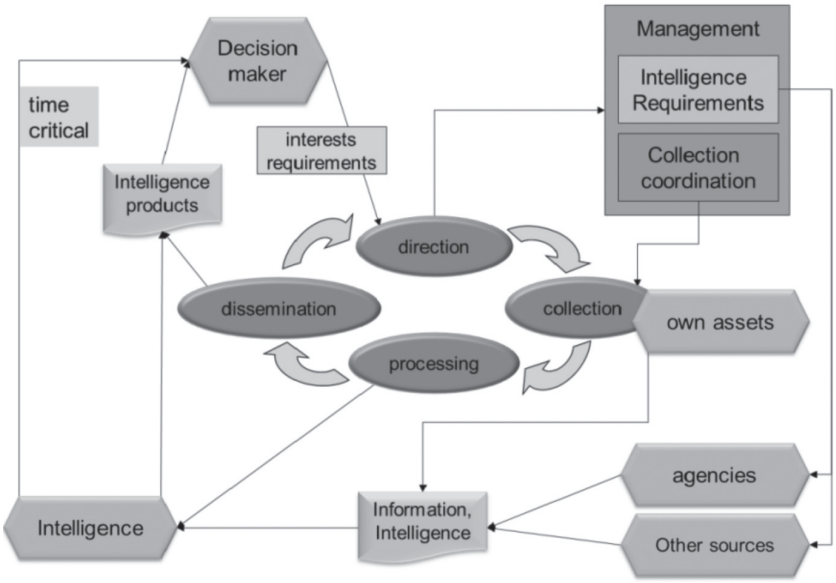
Intelligence is dealing with uncertainties; the more information is cross-checked and subsequently validated or confirmed, the more accurate the assessment will be, in an attempt to decrease as much as possible the number of mistakes, through the intelligence cycle depicted in figure 3.

Information that is needed by and relevant for the decision maker provides through the Intelligence processing an accurate situational awareness [11], [16].

Such a best possible accurate situational awareness is a prerequisite to make appropriate

decisions [9], [11]. The intelligence efforts are driven by the information requirements of the decision maker, who can directly readjust the efforts by giving guidance [11], [16]. As questions always aim to recent developments and changes, information in databases and repositories are never sufficient to respond to the information request. Therefore, a need arises with the decision makers' request to collect more information via the available various collection disciplines [16].

FIGURE 3: THE INTELLIGENCE CYCLE IN THE COLLECTION COORDINATION AND INTELLIGENCE REQUIREMENTS MANAGEMENT (OWN ILLUSTRATION).



It can be summarized that Intelligence is the basis of on which a decision for operational activities is built [12]. Or in other words Intelligence drives the mission. "Thus the intelligence contribution must begin even before operational planning starts."[12]

The cyber domain is reaching into the domains air, land, sea and space as 5th dimension [19]. Reaching implies overlapping areas. This is underlined by the fact that many assets have a position in the physical as well as in the virtual cyber environment [2]. This feeds the assumption that cyber might be a different "view" on or classification of information, data, assets etc. Thus, cyberspace is not really something completely new and we can examine existing traditional information sources and repositories.

It is necessary to take into consideration that although defining cyberspace as an abstract fifth dimension, it is physically based on hardware components [23]. The hardware is used by persons with capabilities with some intent. Therefore, fusing technical data, e.g. derived from raw network packets, with traditional intelligence appears to provide more comprehensive analysis of the cyber threat on a more precise level than before as it includes the human factor, which is per se neglected in any exclusively technical analysis [20], [23].

In short, a technical capability to harm one's systems is irrelevant as long as there is no intent to do so.
If this discrimination process is not implemented, the decision maker will undoubtedly suffer an overdose of possible threats that could paralyze his action. This critical mitigation between risk and opportunity makes the decision making much easier.

Focusing only on technical data that is delivered by physics-based sensors, it must be kept in mind, that sensors can only be put in dominated or at least controlled areas. Otherwise they become vulnerable and can be manipulated [14].
New and/ or actionable knowledge may result from low-level data that became meaningful information by a goal-directed cross-linking of different information products [20], [22].
Finally trustworthy intelligence will be created from this knowledge in a cyclic (intelligence) process [20] that has several iterations and readjustments caused by quality of source and information as well as by cross-checks. In cross-checks often available and potentially conflicting information shall be verified or falsified to confirm a situation. This makes it a time intensive challenge for the human analysts although absolutely necessary in order to avoid misleading conclusions [11], [14].

The traditional security tools that are used in network monitoring are generally only point solutions that provide only a small technical section of a bigger context [20]. Thus, it becomes apparent that the technical data needs to be merged with complementary information [14].
Information elements are generated by different, often heterogeneous sources [22]. They do not only include computer network specific sensors, but also other physical sensors and human sources.
Following [19] in dividing cyberspace into a physical, a logical, and a social layer gives a good first base for the types of information that need to be looked at, further examined and exploited for a more comprehensive situational awareness.

Intelligence, surveillance and reconnaissance in and of cyberspace need to be conducted to "bring light" into uncertain situations and meet the information need.
With the novelty of cyber some introduce in the domain of intelligence the term Cyber Intelligence. If it is used in the sense of 'collecting, analysing and countering of cyber security threat information' it might fall short, especially when the focus lies only on technical information.
The emphasis of the intelligence efforts for Cyber or in short *Cyber Intelligence* is different from those for conventional intelligence operations, also if adversary intent and capability are for both of interest. Cyber Intelligence identifies Cyber Threats on the understanding of the global network and computer architectures and associated threats by analysing and fusing conventional threat data with network information. By merging those with global events the actual technical network border can be penetrated.

At the moment Cyber Intelligence appears to be strictly defined in technological terms by technical experts, what is not in the best interest for the task and needs to be completed by a broader inter-discipline view in order to meet the operational requirements [18].

Missing is the connection between the collected technical data and information that is already available in different traditional established information structures and domains. Thus, we follow [5]'s argumentation that the focus should be on fusing information from multiple sources to learn and analyse the tools, tactics and motives and take a look in the next section to the different disciplines of "traditional intelligence in possible support for cyber aspects [4].

4. INTELLIGENCE SUPPORT FOR CYBER SPHERE

Technical data has often been collected mindlessly and it was tried to make sense of the huge data sets [21]. To find useful information or even intelligence in that enormous amount of data, the strategy of mindless collection and purely technical assessment must be changed. The technical data must be a part of the bigger situational picture that gets information also from the traditional intelligence disciplines for fusion.
We state that in the traditional intelligence fields information is already available or can easily be collected by adjusting the intelligence collection plan.
Therefore it is necessary to take a look at the different disciplines and the conventional data produced and available in them, waiting to be collected and merged with the technical data.
The basic groups of collection disciplines are Human Based Intelligence (HUMINT), Imagery Intelligence (IMINT), Open Sources Intelligence (OSINT) and Signals Intelligence (SIGINT) [12], [16], [24].

In HUMINT data like names, locations, as well as motivations and capabilities are processed. In addition it could be also directed to find WebIDs. As well, HUMINT contributes to the drawing of human networks, thus enabling to understand the possible underground ramifications of an apparently isolated threat.
OSINT can provide host information, IP numbers, information on the used ISP, the location, WebID, homepage(s), blogs etc. It can be done in a technical approach, but also in a more abstract level, e.g. via scanning social media. Associated with HUMINT, OSINT enhances the merging process between the verbally expressed intent and the effective behaviour.
IMINT can provide further information about a location, used infrastructure, types of antenna and possibly about networks, especially in connection with GeoINT, HUMINT and SIGINT.
SIGINT intercepts can not only reveal the transmitted message, but also show the way of data. Thus, further analysis might implicate on top of a physical network a virtual usage network.
GeoINT can bring an invaluable added value to the overall analysis process through their capability to manage large databases originating from various economic fields.
As a summary, any data related to grids is of use, be it servers, data centres, web cafés, that is any facility being assessed to be of interest in the analysis of the cyber threat.
Even though varying from one organization to the other, intelligence reports may be characterized in four categories:

- immediate reports to broadcast brand new information,
- timely reports, which include an assessment and intend to give the heads up,
- ad hoc reports dedicated to one specific issue and
- national intelligence reports.

The latest category is of a peculiar interest in the field of international cooperation, as those documents are the steppingstone for deciding what can be shared or not.
These products usually include analysis of adversaries, their capabilities, objectives, doctrine and limitations [10].
To support the cyber efforts, those products should include information or details relevant for cyber intelligence. That is the case, when they are in relation to the cyber environment, either in the physical or in the virtual cyber sphere. Many relevant intelligence snippets can be found in open sources like chat rooms, postings in forums, blogs and news groups, but also in e-mails, wikis, web sites, social media and messaging communications. By looking for identified buzz-words in a first automated scan and then refining the search taking into consideration further information that is connected to the first results. Those sources are open and thus available and easily accessible. Information from private communication channels in blogs and forums can be obtained, but this by passing control mechanisms, e.g. a registration.
Information from hacker forums is of special interest. There are chances to find commonalities in different attacks by correlating network data. Thus, not only in regards to content-analysis the forums have to be examined deeper, but also network data can be gained by specific collection efforts [21]. Those forums provide rich conventional intelligence, but also cyber specific information as it is distributed via or hosted in cyberspace.

A cyber skilled analyst could merge conventional information/ knowledge and political events with the cyber specific data [21]. He can develop the same intelligence operational picture for the cyber sphere like the one that is traditionally fed from conventional intelligence disciplines. Thus, he can create a more comprehensive understanding of a potential threat or attack by including context and his experience.
As intelligence is looking over longer periods for reoccurrences, the aggregating of data from multiple sources will reveal patterns that are not evident from a single source [21]. Intelligence can be distinguished between tactical, operational and strategic level. Technical data of a machine or in a network segment corresponds to tactical intelligence level [17]. Operational or even strategic intelligence needs to look beyond the bits and bytes correlating and linking activities of maybe years as for Intelligence on that level not so much the single event or a phase of the event is of interest. It's more the cyclic reoccurrence and the pattern that enables to possibly predict further adversary measures.

After an attack a forensic examination of the intrusion artefacts will provide at least a section of the timeline of the attack/ incident, but also technical data for further investigation and intelligence tasking. For example the examination of the STUXNET source code included snippets that were giving hints to where the originators come from.
Starting from an IP that is associated with an attack a lot of information can be collected on a technical level. The IP allows to get e.g. host name, geo-location to identify the physical origin (or last used echelon) of an attack, the ISP that has registered that IP etc. However, as IP addresses can easily be masked or spoofed, the reliability of that information is poor. Therefore, it is up to the intelligence disciplines to provide further information. Who was using the host with the given IP? What WebID was he using for his actions? Exist further occurrences of this WebID, maybe in similar context? Is only one person using the WebID or several persons? Are there other services he is using with this WebID in the internet? Is he using other WebIDs (e.g.

different e-mail accounts, different login names)? Is he using blogs and social media, what information are contained and published there? What motivations and capabilities does the person have to initiate an action that he is now being under examination? What pictures are published, do they contain geo-tags so that through IMINT and HUMINT further information can be gained by a redirection of intelligence/ reconnaissance efforts. If there is enough information the person can be profiled by his customs, locations, used internet services and also his interests, his intent and capabilities.

Also other starting points are possible like data from an investigation or from a signal intelligence measure. An examination and fusion of social media profile data is also thinkable, if indications exist that justify this proceeding.

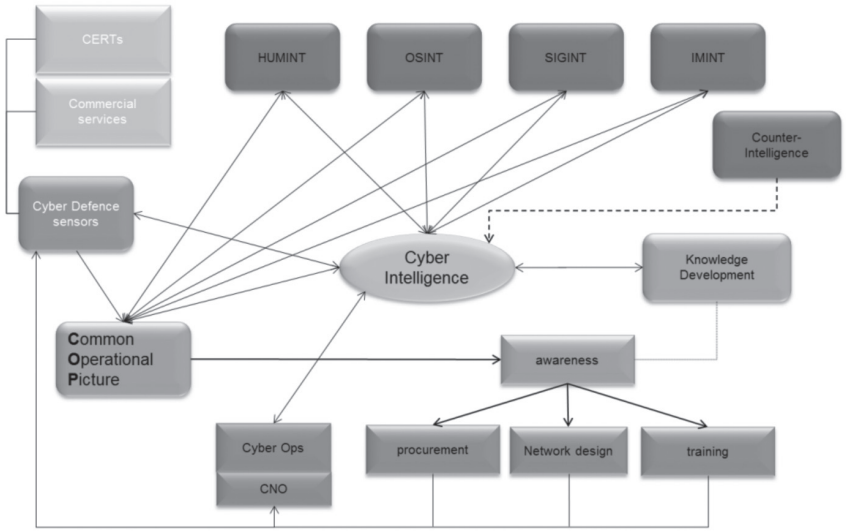
With this approach a professional assessment beyond pure technical evaluation and hypothetical assessments can be made. Fusing the different information from the various intelligence disciplines creates knowledge about the adversaries.

Presenting the relevant information and intelligence in an appropriate way for the receiving audience in order that they can understand the given information and possible effects and results from it, this increases the awareness and causes a better common operational picture serving decision makers as basis for proper and

comprehensive decisions [2], [17]. Better fundamental information can be fed back into the intelligence loop and a more focused readjustment of the efforts by the decision maker is possible. (see figure 3)

For example, an assessment that attacks are not likely at the moment allows the decision makers to turn their attention to more pressing matters [4].

FIGURE 4: VARIOUS SOURCES FOR CYBER INTELLIGENCE, INTERDEPENDENCIES AND POSSIBLE PURPOSES OF USE (OWN ILLUSTRATION)



The gained intelligence must iteratively be exploited and pursued for own objectives. It allows advancing development of own procedures, standards, doctrine and policies. Thus, the findings from analysing the adversaries TTPs and capabilities can be used to adapt own defensive cyber training. In addition it also allows to change passive devices' settings as well as the consideration of the findings in a re-design of the own network or at least in the design of own future networks. They finally should also be taken into consideration in decisions for procurement of hard- and software. (see figure 4)
When technical data and gained intelligence are supplemented with information from the private sector, a very comprehensive picture is created, because commercial/ private/ civil companies/ organisations have other resources and legal constraints. Finally, they are complementary.

5. REQUIREMENTS

For cooperation a common terminology is essential. Only then, there will be clarity among different, probably far away located and maybe even multi-lingual actors. Such a basic understanding is prerequisite for common data analysis in conjunction with all possible intelligence sources and for any following further dissemination of information/ intelligence.
The sharing and exchange of information must be driven by the aim to be better than the status quo by providing effective, timely and actionable intelligence. This allows a comprehensive situational awareness and supports the decision maker in continuous planning and executing Cyber Defence actions. This is achieved by observing and analysing menacing cyber activities and trends [17].
All efforts need to be designed for sustainment. This is underlined by the fact that neither the government, nor the private sector alone can defend against the cyber threat effectively and efficiently. In addition there exist too many approaches to defend everything [21]. Therefore, the efforts must be focused appropriately, which is the main role of intelligence. As developed by Lieutenant-Colonel Foch in his conferences at the French War College, 'economy of forces' consists in selecting where and when forces are to be used the best, instead of trying to face all the possible situations [25]. The cyber threat genuinely and from a purely technical point of view being possibly originating from various locations and using different vehicles, this fine selection of the directions and locations where the cyber defence should focus is of primary importance.
Information and data of penetrations or attacks that are directed against the entire critical infrastructure (CI) are of interest for fusion. By the mainly private nature of the CI and the high interest due to the dependency for governmental functioning, an information exchange between companies and organisations of the CI sectors and governmental institutions will be essential to counter the menace [17]. Neither an intelligence organisation (most are specialised in one intelligence discipline) nor a governmental institution nor a private company can collect, produce or even access adequate intelligence on their own. To keep that status quo will not improve the chance to have reliable data in an environment that has to deal with many uncertainties [1]. Only sharing of relevant cyber threat information will overcome this limitation and enable an informed decision making. For success all sharing partner must contribute. It is not only a "give", but also a "take" liaison. Benefiting from partner's information and intelligence a potentially more complete understanding of the threat landscape can be achieved [1].

A first step will be to cross train cyber and intel personnel in organisations, so that they are able to understand and transfer requirements and limitations of the other work domain.
In consequence, this approach will take the technical based abstract level to a more concrete level, specifying more precisely the attacker. Maybe in the future even an identification and attribution could be possible, when the limits of governmental institutions, international organisations, and civil companies have burst.
Thus, establishing regulations in strategies and policies for the exchange of information and intelligence in the above outlined cyber context is the essential first step in the described process. It must be defined who shares what, with who, under what circumstances, how the information is handled, classified, processed and stored [1]. These regulations are necessary, because on the one hand there exists no broadly accepted standard for sharing information or even intelligence across agencies or private companies. On the other hand – mentioned for completeness – trust is the key for increasing the sharing behaviour. Trust for the exchange occurs at the individual and organizational level [26], [27]. It is the degree of confidence to handle the information/ intelligence with the same sensitivity. Only then the exchange will take place. As well, cooperation between sovereign states is to be fostered for a better efficiency in cyber defence [18].
Agreements between organizations, agencies and private companies and the consequent, augmenting exchange of information are a way to build this trust. On the individual level it is the personal relation, or better interpersonal confidence between the subject matter experts that builds up trust over time and generates consistent and positive effects.
A combination of both is established when institutions are created that host several representatives of different institutions and they meet in order to exchange and merge information [23]. On top of the organisational trust this promulgates the individual one.
The agreements for an exchange of information are not only basis to build this trust, but also necessary to formulate the regulations and control mechanisms as well as the interoperability needs.

6. CONCLUSION

The purely technical data feed is always there and therefore certain. However, now uncertainties have to be accepted and dealt with, when information is merged in cooperation with the intelligence community and other information providers like CERTs. We have shown that persistently consolidating data from disparate sources into meaningful and complementary information allows better and more precise assessments about an adversary's capabilities, his intent and his location. This enhances the cyber situation-awareness and allows a more extensive situational cyber picture.
Those resulting details are actionable intelligence (with all the uncertainties being inherent in such assessments) that allow not only after action or tactical situation updates, but predictive, strategic warning in regards to cyber threat activities. Thus we get away from a purely reactive and defensive position to a foreseeing, flexible, proactive one.
The analysis and fusion of the technical and (geo)political events remains rooted in each analyst's experience, background, and expert opinion. Therefore, providing clear intelligence to the analysts is essential to prevent erroneous conclusions finding their way into the situational awareness.

Of new importance are intelligence, surveillance and reconnaissance operations across multiple intelligence disciplines in the context of cyber. Those operations and methods have not changed, they must only be adapted to the cyber sphere. This requires that the cyberspace is better understood and processes take special properties of cyberspace into consideration.
Same is true for sharing cyber intelligence and cyber threat information: Though we have established agreements and mechanisms to exchange conventional information and intelligence, the supposed novelty of cyberspace and specific properties of the cyber sphere hinder the sharing and exchange of that information.
The national and international organisational structures need to adapt to the new challenges and needs.
Our approach helps to create awareness for the correlation requirements of information of the cyber sphere and the traditional intelligence disciplines.
Further research will have to address who shares what, with who, under what circumstances, how the information is handled, classified, processed and stored; also if the trust question is still not solved.
In the exchange of that valuable fused information rests a high potential to shift the balance between attacker and the defender [1].
Fusing the complementary information to actionable intelligence allows decision makers better to prevent surprise attacks in Cyberspace and the way we respond. The information "nuggets" are out there waiting to be collected.

REFERENCES:

[1] S. Barnum, Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™) [Online]. MITRE Corporation, 2012. Available: https://msm.mitre.org/docs/STIX-Whitepaper.pdf
[2] M. Lanham (2012), Operating on unconventional Terrain - Cyber Defense Planning [Online]. Army Communicator. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a571985.pdf
[3] C. v. Clausewitz, On War [Online]. Available: http://www.gutenberg.org/files/1946/1946-h/1946-h.htm
[4] J. Healy and L. van Bochoven (2012), Strategic Cyber Early Warning: A Phased Adaptive Approach for NATO [Online]. Atlantic Council. Available: http://mercury.ethz.ch/serviceengine/Files/ISN/155419/ipublicationdocument_singledocument/22f57269-9d44-4cac-ac21-21423273e1d1/en/NATO+Cyber+Warning+2012.pdf
[5] M. David and K. Sakurai, "Combating Cyber Terrorism: Countering Cyber Terrorist Advantages of Surprise and Anonymity", Proc. IEEE AINA, pp. 716 – 721, 2003
[6] M. Mateski et al., "Cyber Threat Metrics", Sandia National Laboratories, SANDIA REPORT SAND2012-2427, Unlimited Release, 2012
[7] O. Kempf, in: Introduction à la Cyberstratégie. Chapt 6, pp. 78-99. Economica. 2012.
[8] M. Osorno et al. (2011), Coordinated Cybersecurity Incident Handling - Roles, Processes, and Coordination Networks for Crosscutting Incidents [Online]. Available: http://dodccrp.org/events/16th_iccrts_2011/papers/189.pdf
[9] W. Koch et al., "The JDL Model of Data Fusion Applied to Cyber-Defence – a Review Paper", Workshop on Sensor Data Fusion - Trends, solutions, Applications. IEEE. 2012
[10] E. M. Hutchins et al., "Intelligence-Driven Computer Network Defense - Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", Proc. of International Conference on Information Warfare & Security, pp. 113, March 2011
[11] G. Thibault, "Intelligence Collation in Asymmetric Conflict: A Canadian Armed Forces Perspective", Proc. IEEE FUSION, 2007
[12] The Joint Staff, United States Army, "Joint Publication 2-0: Doctrine For Intelligence Support To Joint Operations" [Online]. Washington D.C., 30 june 1991. Available: http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/

[13] F. Cheng et al.: RemodelingVulnerability Information; in F.Bao et al (Eds.) : Inscrypt2009, LNCS 6151, pp. 324-336, 2010 ; Springer Verlag Berlin Heidelberg 2010
[14] M.A. Pravia et al.: “Generation of a Fundamental Data Set for Hard/Soft Information Fusion”, Proc. IEEE FUSION, 2008
[15] S. Dossé: Le Cyberespace, Nouveau Domaine de la Pensée Stratégique. p.119, Economica, 2013.
[16] A. Koltuksuz and S. Tekir, “Intelligence Analysis Modeling“, Proc. IEEE ICHIT, Vol. 1 , pp. 146 – 151, 2006
[17] B. Norquist, “Governmental Effects upon the Cyber Security Decision Making Cycle” , SANS Institute, White Paper, 2005
[18] “French White Paper on Defence and Security” [Online], 2013. Available: http://www.gouvernement.fr/sites/default/files/fichiers_joints/livre-blanc-sur-la-defense-et-la-securite-nationale_2013.pdf
[19] United States Army Training and Doctrine Command, “ The United States Army’s Cyberspace Operatins Concept Capability Plan 2016 - 2028”, TRADOC Pamphlet 525-7-8; 2010.
[20] S. Jajodia et al. (Eds.), “Cyber Situational Awareness”, Advances in Information Security, Vol. 46, Springer Verlag, 2010
[21] S. Goel, “Cyberwarfare connecting the dots in cyber intelligence”, Communications of the ACM, Vol. 54, pp. 132-1408, august 2011
[22] J. Sander et al., “ISR Analytics: Architectual and Methodic Concepts”, Workshop on Sensor Data Fusion: Trends, solutions, Applications. Pp 99 – 104, IEEE, 2012
[23] R. Clarke and R. Knake, Cyber War, Harper Collins, New York, 2010
[24] E. Rosenbach and A. J. Peritz, “Confrontation or Collaboration? Congress and the Intelligence Community”; The Intelligence and Policy Project; Belfer Center for Science and International Affairs; John F. Kennedy School of Government, Harvard University; 2009
[25] F. Foch, Conférences faites à l’Ecole Supérieure de Guerre [Online], pp. 46, 1903. Available : http://gallica.bnf.fr/ark:/12148/bpt6k86515g
[26] J. V. Treglia, “Towards Trusted Intelligence Information Sharing”, Proc. ACM, SIG KDD, Workshop on CyberSecurity and Intelligence Informatics pp. 45-52, 2009
[27] S. Ritter, „Computernotfallteams: CERTs als zentrales Element nationaler Cyber-Sicherheit“, BSI Forum, Nr. 6, 20. Jahrgang, 2012