Technical Evaluation Report

G. Wyman
2 Palmer Gardens
Wivenhoe CO7 9FL
UNITED KINGDOM

glyn.wyman@gmail.com

ABSTRACT

This paper presents the findings of the Technical Evaluator of the Symposium Cyber Defence Situation Awareness held 3rd and 4th October 2016 in Sofia Bulgaria. A summary of each presentation is included. It concludes that visualisation of situation awareness requires further research and that cyber events need to be presented in a timely fashion coupled with their impact. Several potential models, based on graph theory, to analyse the situation are discussed with the respective displays.

INTRODUCTION

Any commander requires an up to date assessment of the operational environment, including any cyber effects presented in a coherent form. Cyber is now generally recognised as the 5th operational environment but has very different parameters to the more conventional land/sea/air/space environments. In particular the transition from benign to hostile status is ill defined and the impact on the general populous unknown. The aim of the symposium was to bring together experts and practitioners to discuss the state of the art to achieve a succinct representation of the environment to establish situational awareness.

An IST sponsored Working Group had prior discussions over a period of three years and have used this forum to present their findings. The chair of the Working Group also chaired the symposium and had support from the members.

Cyber-attacks are all pervasive, demanding collaboration from all sources, the expansion of smart mobile phones and the use of applications to control everyday events compounds the risks. Targets range from sophisticated control systems with ad hoc protection to commercial devices with no inherent defence.

THEME

Topics for discussion in presenting a timely and appropriate Situational Picture were:

Cyber Defence

Situation Awareness

Cyber Resilience

Current Challenges in Cyber Security

Security Metrics

Dynamic Risk Assessment

Mission Assurance

Continuous Monitoring

Network Analysis and Monitoring

Cyber Defence Visualization

Visual Analytics

Cyber Security Models and Architectures

Security Verification, Evaluation and Measurement

PERCEIVED MILITARY ISSUES

Situational Awareness is a necessary aspect for a commander but it is essential not to overburden the individual with unnecessary detail. The specifics presented will be dependent on the environment but also on the prior knowledge and experience of the user. Ideally tailored to the individual but this may not be possible and a generic form should be presented as a default. The nature of cyber-attacks cannot be predicted and adversaries devise new methods as we counter observed events. Defensive measures which are reactive will always exhibit a delay and will be behind the curve of influence. The latency permitted to defend against a probe, to minimise damage, demands that automatic counters are required. Reactions instigated by artificial intelligence (AI) need to be sanctioned at some stage and the consequential impact assessed.

Cyber operations are regarded with high priority and established as the 5th Operational Environment. Knowledge of future tactics which could be employed is sparse and the speed of any attack extremely high. Cyber as a weapon of war is a relatively new concept and rapidly evolving with technology. The potential impact is enormous and the disruption to normal life considerable. A commander needs direction to identify an anomaly indicating an attack with the consequential inference to hand. This is made more difficult by the dynamic nature of the adversary with no well-defined location. Some defensive measures may provoke probing from a different vantage position which could exacerbate the position. The vulnerability of some assets particularly autonomous agents is significant, measures to improve their robustness could reduce their efficiency and hence their capability. Trust in the system is paramount.

EVALUATION

Facilities

The room was well appointed with the delegates sat in rows with full visibility of the screen and adequate acoustics. WiFi access was provided giving access to the STO website and other internet facilities allowing the delegates to view the papers which had been uploaded by the secretariat prior to the symposium. Coffee was served during the breaks with ample opportunity to engage with the presenters to elaborate on the research and to seek points of clarification. I observed very productive discussions in the breaks. In addition an exhibition was arranged by AFCEA to enable relevant companies from Bulgarian to show their capabilities. A buffet lunch was provided to enable discussion with the companies to continue during the lunch breaks; an augmented reality demonstration was available to experiment with and inject their own items.

Overview

Situational awareness is essential but difficult to achieve particularly when collaboration with all disciplines is demanded. The military commander needs to be alerted to infrastructure activity and any adverse effects on commercial entities coupled with the projected social impact in addition to the disposition and status of his military assets. The topics addressed in this symposium were understandably biased towards the military domain but some of the methods identified could be applied to commercial aspects. An initial attack could appear innocuous but the secondary effects may be rather more intrusive. Cyber activity has been observed over a number of years but the processes adopted remain immature.

My initial reaction to reading the papers was that the subject was treated in a superficial fashion but on reflection the detail exposed the current state. I suspect that the specifics for this topic for example applying deep learning and other artificial intelligence could not be presented in this forum, however, since commerce is inherently involved, wider exposure should be encouraged. Some of the work takes leverage from commercial solutions which are to be encouraged with the necessary constraints needed to allow a dialogue; of particular concern is the ease with which risk reports will be disseminated. A number of the solutions make extensive use of modules from other applications, whilst this is efficient in reducing time, weaknesses in the code are propagated. Four keynote speakers provided the appropriate background and presented a) the policy adopted within NATO Headquarters, b) a means to reduce procurement time, c) a national perspective and d) the necessary cooperation with industry. Some duplication in the presentations was inevitable but time did not permit prior mutual review. It is to be encouraged that a paper is associated with the keynote speeches to ensure a viable reference. All four provided background to the topic, a necessary input but did not advance the science. A reduction in the number of keynote speakers should be addressed.

The papers, received for the symposium, were divided into four sessions consistent, with the declared topics in the call for papers: CDSA Architectures and Approaches, CDSA for Mission Assurance, Security Metrics for CDSA and Visual Analytics for CDSA Some topics identified in the call for papers were not presented, specifically associated with security but this did not detract from the overall value.

CDSA Architectures and Approaches: In this session it was recognised that diverse parties have a different interpretation to the terms used and that common definitions need to be established, particularly to ease collaboration. Highlighted is the boundary of Situational Awareness; one paper considered the decision process to be external to SA whereas the majority included the decision aspects to allow the appropriate feedback and hence close the loop. The impact on the general populous introduces a socio-technical element not encountered extensively in earlier analysis. Techniques based on software defined networks (SDN) and compared with the OODA loop were presented with a preference for SDN. Trust was raised and the associated authentication which itself should be a defensive measure. Expanding the network to include private networks is seen as needing thought. It is impossible to design a system devoid of error and as such the architects must take cognisance of the shortfalls.

CDSA for Mission Assurance: Two papers were presented in this session addressing the resilience of any SA system. The first constructed a model using probabilistic inference to focus on mission uncertainty. Aggregation of conditional probabilities provides an output which is readily understood. The second covered a whole raft of applications offering a rapid requirements analysis tool. Assurance and authentication are crucial to the confidence a commander can place in the information available which will colour his judgement and provided quantitatively in the models.

Security Metrics for CDSA: A data centric approach was advocated utilising the experience and tools available in handling massive data sets and accommodating different vendor security products. An emphasis was placed on priority for mission systems cf. reacting to vulnerabilities. A whole series of dashboards were presented, some with a geospatial background offering risk assessment in coloured form. The effects of mitigating actions were displayed. It was proposed that a concept of cyber health be instigated but would require input from private companies which could be difficult. The Netherlands has a scheme in which participation is encouraged but once a member cannot resign. The fragility under stress is a parameter of interest which can be derived using the Harsupex suit of programmes which were presented. A demonstration of the potential to develop models to support the decision process and present situational awareness was provided.

Visual Analytics: Visual analytics is a key enabler for information display and it is essential that what is presented is succinct and relevant to the user. A large number of options were offered with the associated queries of the data repositories. The standard forms of the dashboards were supplemented with 3D representations and immersed reality. The fusion of the physical plane and the cyber plane offered an

interesting process. Extensive software is available to implement the general displays but increasingly greater requirements are indicated for more customised displays with automated elements; the later to accommodate the short time scales involved. The long term aim is to present the commander with the situation, the implications of any anomaly, and the impact on the options to counter the observed event.

Feedback from TER Presentation

A part of the TER presentation to the IST Panel included areas where it was thought improvements could be made to bolster the reputation. We appear to be running under the cusp and achieving satisfactory symposia when a little stimulus could achieve a much higher standing. The first suggestion was to achieve a publication which could be indexed or collaborate with a journal already in this category. Reaction from the floor was positive and several relevant publications named. The impact could be considerable with additional time for peer review coupled with higher level of administration. In principle peer review should be applied already, but time scales and other schedules have allowed only limited recommendations to improve the papers. The depth of technical detail needs to be improved although the amount of rigour will be dictated by the target audience. A means to encourage younger scientists was postulated involving offering seed monies in return for writing a paper. Some National Bodies already support academia in this fashion and have reaped benefits. A suggestion from the floor was to make a video recording of the proceedings which would be available over the internet. In some conferences this has been tested and shown to have some merit. STO was reluctant to offer this facility but would consider ad hoc requests.

Analysis of Questionnaires

I received 17 completed questionnaires from which the following is derived:

All respondents marked the symposium as worthwhile with 42 percent giving the highest mark. The theme of the symposium was generally acknowledged to be very appealing and topical with 35 percent reducing the assessment to satisfactory. Most of the papers met the objectives and were regarded as satisfactory with one of the respondents viewing the content as too superficial. Not all the speakers were perceived as entirely organised and the quality of the visual aids marked down. One reply indicated that the speakers had been allocated too much time in comparison to the 95 percent who thought the time allocated appropriate. The same distribution is observed for the discussions with the outlying point indicating too short a time. The overall value has been computed as 86.7 from a maximum of 100 with the overall assessment giving 47% excellent 20% very good and 33% good. One comment encouraged stronger involvement with persons outside the STO community, a second thought the keynote speakers offered a superficial presentation coupled with a low number of papers, which was countered by another delegate giving a keynote the most interesting paper.

Presentations

The chair of the IST Panel John Mc Lean opened the proceedings and provided a brief overview of the STO and the position of IST within this body. The disciplines addressed in The Panel and some of the work in hand was presented. Full detail of the structure and the associated activities is available from the RTO web site. The hosts then welcomed the delegates to Sofia and wished for a successful meeting. Douglas Wiemer as chair of the symposium started the proceedings. The following is a summary of the papers; inclined readers are directed to the RTO web site to establish detail where the papers are available to download.

Keynote 1: NATO Cyber Defence Post Warsaw. Christian Lifländer

The significance of Warsaw is where the decision was taken to regard cyber as the 5th operational environment. The impact on policy decisions is considerable, cyber actions are not constrained by political boundaries and society is exposed to unconstrained risk. No preconceived defence is envisaged with adaptive

detection employed. The availability of proactive defence mechanisms and their use needs consideration both ethically and legally. Nations have differing views on internet sovereignty and whether cyber-attacks are comparable to physical attacks. Collaboration with private companies to cross match dependences is advocated. Regrettably a reluctance by politicians to invest significantly has been observed potentially because attacks are yet to result in direct loss of life, to date published attacks have resulted in financial loss or release of personal data. The need for resilience was emphasised

Paper 1: Understanding Cyberspace through Cyber Situational Awareness: Bob Madahar

This presentation provides an hypothesis for cyberspace understanding and identifies areas where further work is required. Collaboration is critical to achieve a defensive posture requiring that all parties understand the terms used. The conjecture that cyberspace is wider than the internet was made and requires agreement and should be addressed as a socio-technical system of systems. The need to support a cognitive layer was emphasised. A comparison was made between the Endsley model and that used in the UK. The challenges identified included: a) the complexity of handling intangible artefacts, b) persistence and pervasiveness, c) big data, d) tracing cyber inadvertent events, e) establishing sufficient comprehension and judgement to achieve foresight. Identified avenues to progress included: tracking of propagation effects, fused SA, applying automation and deep learning.

Paper 2: Leveraging Software Defined Networking (SDN) for Cyber Situational Awareness in Coalition Tactical Networks: Franck Le

The premise that trust is limited in a coalition environment leads to a more cautious approach and the distributed algorithms employed further increases the risk and vulnerability. The ability to present a SA picture is achieved by applying a modified OODA loop with separated control plane and data transfer. Observe maps onto performance metric Orient to analyse with Decisions taken using graph theory. The work is in its initial stages but shows distinct promise.

Paper 3 Examining Correlation Techniques to Improve Strategic Decision Making through Advanced Cyber Situational Awareness: Preston Frazier

Describes the development of a common operational picture evolving from the traditional Geospatial heat maps, Network graphs and IP-Space Hilbert maps. The need to develop an alternative is necessary to overcome the faults inherent in the earlier applications. The resultant Hierarchical IP-Space maps were presented for particular scenarios and shows promise. The software will support user defined meta data to tailor the displays within the dynamic environment. It can be extended to support sharing of the situational awareness for multiple stake holders.

Keynote 2 Scenario Driven Capability Development Reginald Sawilla

The inertia of procurement processes does not match the requirements to have systems deployed in a time scale applicable to cyber activities. The speech outlined the process adopted to accelerate the procurement for a Cyber SA tool to be deployed by NCI Agency. Industry representatives who had responded to the initiative were present at the symposium and gave support to the initiative. In essence selection is made with greater involvement by the companies to develop a better understanding of the desires behind the specification.

Paper 4: Probabilistic Mission Defence and Assurance: Alexander Motzek

A model has been developed which provides an output in linguistic form readily understood by third parties. The focus has been on retaining mission functionality and understanding the impact in statistical values. The probabilistic approach accumulates information from a variety of experts and using well tried mathematical

techniques aggregates the inputs. A question was raised as to when the underlying graphs become intractable during the optimising process, it is known that the problem is np complete but heuristics can be adopted to treat practical problems.

Paper 5: Mission Dependency Modelling for Cyber Situational Awareness: Steven Noel

The presenter from Mitre is part of the adjudication process within the NCIA. The models described will be incorporated in the November 2016 initiative by NATO to demonstrate CDSA capabilities. Mitre has a number of tools currently used by Government Customers including CyGraph an analytic tool using flexible graph analytics allowing ad hoc queries, The graph tool will handle AND and OR functions in the description of the edges and capture human behaviour cf technical functionality. Detail not provided during the symposium.

Paper 6: Evolving Continuous Monitoring to Cyber Situational Awareness: George Romas

This presentation is a candidate for the CDSA and shows extensive flexibility to accommodate diverse data sources and display the results on a wide variety of dashboards. It is a data centric approach allowing security products from different vendors to be accepted. It incorporates trusted internet connections and is based on a private cloud.

Paper 7: Cyberspace Security Threats Evaluation Systems of the Republic of Poland: Przemyslaw Berezinski

A national perspective reacting to the NATO recognition of cyber as a domain and the EU directive declaring that cyberspace needs to be monitored with the goal to achieve CDSA at a country level. Project CyberEva is an initial model to meet the aim. The model is a weighted directed graph used extensively in other disciplines and with a strong mathematical basis. Risk assessment is displayed in colour form with the exampled shown on a geospatial canvas. It has the capability to show the effects of different mitigation strategies. As with all SA models collaboration is essential but it was shown to be difficult to obtain data from Private Companies. The assessment tool will investigate cyber capabilities and vulnerabilities and hence establish cyber health.

Paper 8: Metrics for Cyber Robustness: Fabrizio Baiardi

The presentation describes a suite of programmes to establish if a system will survive a sustained attack. The initial conditions are an attacker who can select the optimum escalation strategy to reach a goal and design alternatives en route. The attacker is characterised by its initial knowledge and so can emulate an internal attack by giving extensive initial knowledge. Human intervention is minimal. The output isolates an attacker and the critical nodes identified. The confidence in the outcome is defined by the number of trials. The current model requires 10,000 repetitions to achieve 95% confidence. There is no closed form for the stress level making validation difficult but the results are consistent with the results obtained under trial conditions during Locked Shield

Keynote 3: Role of Non-Governmental and Professional Organisations in Building Cyber Security Awareness in Society: Konstantin Zografov

A high level presentation emphasising the need for awareness of the Cyber capabilities of an adversary which are documented in a AFCEA white paper ‘Driving Cybersecurity HOME’. He also highlighted a general tool ‘Balbridge’ to enable users to better understand their cyber risks. The view expressed was that the general public will not comprehend the value of security unless they have a complete appreciation of the risks, education and exposure to the issue is paramount.

Paper 9: Service Measurement Map for Large-scale Cyber Defence Exercises: Mauno Pihelgas

The description of the tool used extensively to assess 'Exercise Locked Shields'. The requirement is to provide analysis of the performance of 20 teams during an exercise; commercial tools were considered but did not meet the requirements. The tool uses a Nagios core with a Selenium WebDriver coupled with custom agents. Feedback from the users has been positive but further refinements have been identified. Several examples of the visualisation assisting the analyst to identify anomalies were presented.

Paper 10: Achieving Cyber Situation Awareness through a Multi-Aspect 3D Operational Picture: Salvador Llopis and Wim Mees

The paper expands on the work as part of the contribution to the IST-108 Working Group and shows a presentation which is succinct and intuitive. Size, colour, position, intensity of colour and motion in a 3D representation all have significance and the user is rapidly drawn to the salient aspects. The model is based on a Mission Asset Control (MAC) triangle and applies the coupling between the bodies. Domain knowledge is captured in Fuzzy Logic form with multiple metrics available for use in both hard and soft form. It was recognised that objective validation is required and that collection of the necessary data may be a challenge.

Paper 11: Cyber Common Operational Picture: A Tool for Cyber Hybrid Situational Awareness: Israel Perez

The group stated with the laudable aspiration of predicting patterns of activity. The basis is again graph theory coupled with complexity theory. They develop three planes Physical plane, Cyber plane and a Hybrid plane. The fusion model operates in the hybrid plane to draw inference from the physical sensors and the cyber reports. The system known as CyOP allows different visual perspectives including 3D models, virtual reality and immersive virtual reality; shown as slides during the presentation.

Paper 12: Big Buttons: A Situational Awareness and Cyber Defence Solution: Dawn Starling

The presentation presents the current position on the companies' aim to support the NCI Agency within NATO-MN-CD2. They have integrated a suite of mature COTS packages to allow the integration of the declared data sources; it would appear sufficiently flexible to accommodate new sources. Good quality data is declared as the core and stored in a cyber data warehouse. Visualisation techniques can be customised with ad hoc searches and alerts on declared thresholds. Again a large number of dashboards were presented which could be readily tailored.

Keynote 4: National Cyber Picture and Collaborative Resiliency George Sharkov

The National Cybersecurity Coordinator presented the Bulgarian take on the cyber issues. He addressed the increasing dependence of society on the digital age and emphasised that resilience is a critical aspect. Industrial control systems in particular are declared to be vulnerable and correction is difficult with patches. He acknowledged the known unknowns as mapping to cyber security but also that we should prepare for the unknown unknowns to maintain resilience. We should engage with all parts of society and except that recovery may identify a new state. The aspect that aggregation may compound the stress was observed.

Paper 13: Achievements and Outcomes of IST-108 Task Group, Cyber Defence Situational Awareness: Douglas Wiemer

The chair of IST-108 and of this symposium are the same person which allows the outcome of the Working Group to advertise their findings and analyse related work by scientists external to the group. Refinement is possible before the findings are published later this year, details will be available on the STO website. The inclined reader is also directed to the earlier published work on the topic specifically: IST-081, MSG-117, SAS-106, IST-110 and IST-117. They intend to report on innovative approaches, application of various

methodologies and the comparison of different control loops. We were privileged to have a pre-view of their analysis

Round Table Discussions

The schedule allowed for a period of consolidation and for the delegates to clarify specific detail. Regrettably an alternative meeting was arranged reducing the number of participants. The following comments were made:

a) Take advantage of the status afforded by the declaration that cyber is regarded as the 5th Operational Environment. To achieve any major benefits those making policy decisions and the commanders need an understanding of the effects and the implications on both the environment and society. Education and collaboration are key elements.

b) Ensure stronger collaboration between the EU and NATO. The fact that cyber is all encompassing implies that collaboration is required with all parties including Private Industry, Banking Sector and Government.

c) A concern was raised about the way people react including the impact of the socio-technical system-of-systems, identified in an earlier paper. A comment was made that since no cyber action is yet to record a direct loss of life reduces the interest. Once loss of life is reported it may focus the attention.

d) The aspect that we are currently reactive to probes leaves us retarded with respect to aggressors. Predicting behaviour is notoriously difficult and covering software development in operating systems and applications to ensure no loop holes can be exploited even more difficult. A study to identify 'bad behaviour' was advocated but raises the demand to characterise normal behaviour which may be context sensitive.

e) Quantify the role of machine intelligence and set a threshold at which mitigation action is displayed for consideration. Aspects of deep learning, and the impact of probing on learning algorithms, needs to be investigated.

f) The rate at which aggressive action has an impact, and can propagate, on a system is considerably increased compared to other domains. The need to reduce false positives was acknowledged for any monitoring system.

g) We need to manage expectations of the systems considering the investments made. An acknowledgement that some disruption is inevitable unless more monies are available to analyse the systems needs to be expressed.

Exhibitors

AFCEA had organised a group of local industry, loosely involved with cyber, to present their companies during the breaks. For details, please contact the company directly a brief outline recognising their contribution is made bellow:

1) ICB Software and Consulting: Provided an augmented reality demonstration which the delegates could exercise. Offered a facility to scan USB sticks and prevent laptops reading the corrupted files.

2) Atlantic Technology: Closely associated with their parent located in Israel. Develop high tech security orientated products.

3) Miltech Ltd.: Is a partner with a large number of international companies and is involved with a number of projects with the Bulgarian Ministry of Defence.

4) Telelink: Recently completed an automatic data collection for a Bulgarian infrastructure project.

5) Esri: Developed a tool ArcGIS to support for Military operations and have written a white paper on a Geospatial approach to cybersecurity.

6) Lirex com: Offering Network Security, Database security, Mobile Device Management and Increased security level.
7) Intracom: A global company with expertise in streaming petabytes; also involved with data centred visualisation and network design.
8) Techno Logico: Develop a comprehensive range of information technology services.
9) Verint: Provide a secure capability employing digital equipment from various disciplines, ip cameras video analytics etc.
10) Electron Progress: Project management company with appropriate clearances they have worked with The Ministry of Defence in Telecommunications and Security for a number of years.

CONCLUSIONS

The Symposium met the aims declared in the 'Call for Papers' and provided a forum for scientist to exchange views and techniques. The content of the papers is variable in detail and rigour as would be anticipated, but reflects the current position of research in the open. Likewise subject matter shows a bias towards modelling and visual analytics compared with the security impact. The dynamic nature of the environment coupled with the effects on a wide range of disciplines forces continual research not only in displaying the attack but also indicating the impact on systems.

The models presented were based on graph theory but this should not be pursued at the expense of other techniques. A raft of dashboards are available to assist the analysts but succinct methods must be adopted, 3D representations and augmented reality are candidates for consideration. Graphs with the edges defined by the associated conditional probability showed promise to predict the impact on the environment and the socio-technical system-of-systems. Populating the values and characterising the human reactions needs expert input and extensive research.

I commend the Chair and his technical committee for a successful outcome, declaring the status of the discipline and identifying areas where refinement and new avenues need to be explored.