Foundations for modelling conscientious attacking in electromagnetic cyberspace

Nigel Davies
Faculty of Science and Technology
Bournemouth University
Bournemouth, UK
ndavies2@Bournemouth.ac.uk

Huseyin Dogan
Faculty of Science and Technology
Bournemouth University
Bournemouth, UK
hdogan@Bournemouth.ac.uk

Duncan Ki-Aries
Faculty of Science and Technology
Bournemouth University
Bournemouth, UK
dkiaries@Bournemouth.ac.uk

Nan Jiang
Faculty of Science and Technology
Bournemouth University
Bournemouth, UK
njiang@Bournemouth.ac.uk

Chris Williams
DSTL
UK
cwilliams@mail.dstl.gov.uk

***Abstract*— Conscientious military attackers deciding to perform targeted Electromagnetic attacks have an ethical problem because their actions may adversely impact non-target victim systems. Their decision-making process should account for the assessed risk to victim systems before engaging in Electromagnetic attacks. In short: Risk-Informed Decision-Making within a complex, dynamic, uncertain environment involving Systems-of-Systems is essential. But how is the related risk assessment performed? This paper identifies some important foundations for modelling this context.**

Keywords—Risk Assessment, Ontology, System-of-Systems, Electromagnetic Attack, Cyber Warfare

I. INTRODUCTION

Much of the field of security and resilience of critical assets in critical infrastructure focuses on defender's perspectives of threats. Defenders are typically operators managing engineered defences of critical assets. The field that this paper addresses is focussed on a unique, specific, perhaps niche area, that considers an attacker perspective within a potentially controversial topic: i.e. conscientious attacking in electromagnetic (EM) cyberspace. Such attacks are associated with EM Warfare and Cyber Warfare.

As Thompson explains [1], whilst the areas of EM Warfare and Cyber Warfare have similarities (e.g. they both aim to degrade enemy systems e.g. Radar installations), there are also key differences because EM warfare has targets and potential victims whereas Cyber Warfare only has targets (unless performing Distributed Denial of Service which is illegal so thus not a legitimate tactic). Although, as Thompson further highlights, there are blurred overlaps. One example is where EM is used as part of the cyber-attack. It is this niche area of cyber-attack using EM signals that this paper focuses on.

EM attacks are where an attacker attempts to sufficiently degrade a target (enemy) system such that its functionality is denied to its operators. The attack approach is different to cyber-attacks which often rely on infecting (with malware) target systems that are then remotely manipulated by attackers. In both cases though, the target system may be degraded. A key important point to note though, is that in EM attacks, the physics of EM signal propagation infers that other non-target systems (e.g. surrounding constituents in a battlefield System-of-Systems (SoS), comprised of civilian EM systems including Critical Infrastructure) could also be impacted and degraded. In other words, EM signals aimed at an enemy target may also degrade other systems (called here victims). The attacker is then potentially determining the operation of such systems. Fig. 1 illustrates an example scenario.

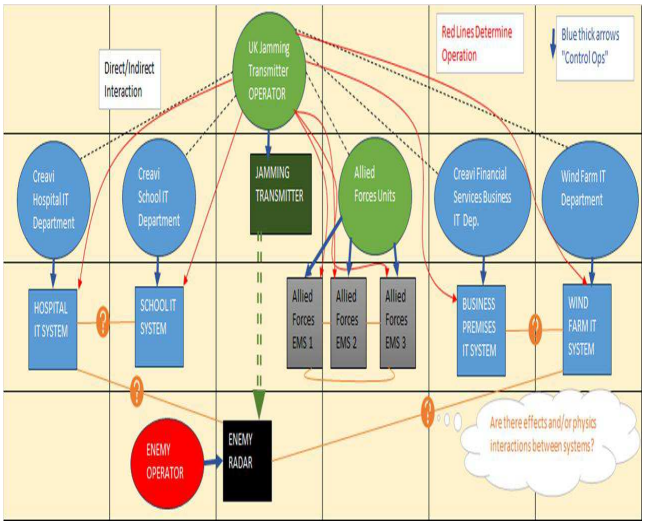

Fig. 1. Example EM Attack scenario

If the level of degradation creates a noticeable impact on victims, it may cause operational consequences for those dependent upon such systems. For example, if the victim is a hospital or some form of critical infrastructure the impact of degradation may become intolerable thereby causing potential chaos to the reliant operations. For those attackers who are not conscientious, this may be of little concern, however, for conscientious military attackers (deciding to perform targeted EM attacks) their decision requires consideration of victim system impacts. This decision-making process therefore should account for the assessed risk to victim systems before engaging in the EM attack. In short: Risk-Informed Decision-Making (RIDM) is essential.

Performing RIDM in such an environment is complicated because victim systems will be complex consisting of Cyber Physical Systems (CPS). Some victim systems may interact with others forming a diverse SoS, thus adding to the complexity. Additionally, victim systems are seldom static so the environment is dynamic, plus knowledge of victim systems may be only fuzzily known to attackers. The RIDM is therefore performed within a complex, dynamic, uncertain environment. But, how is such RIDM to be performed? To address this question, this paper discusses some methodological considerations for how to potentially use mathematical modelling concepts capable of dealing with some of the fundamental issues relating to the calculation of victim risk to aid the RIDM process. To this end, the paper first considers the state-of-the-art in the field of conscientious cyberspace attacks (perhaps using RIDM) and describes EM attacks in more detail (section II). It then discusses a potential approach to relevant RIDM (section III). The nature of the data requirements for such related risk calculations can be described using an ontology and this is discussed in section IV. Section V utilises SoS Theory for modelling EM Attack scenarios. Conclusions are drawn in section VI, by describing significant and novel contributions, highlighting how these contributions advance the state-of-the-art.

II. Review of Current Knowledge

The literature search attempted to discover current knowledge encompassing conscientious cyberspace attacks (whether using EM or not) in order to gain perspectives on approaches to modelling victim risk and the associated RIDM. A search for literature initially focused on attacker perspectives when performing cyber-attacks that involve victims. These are typically Denial-of-Service (DoS) or Distributed DoS (DDoS). The review was performed using the SCOPUS database.

Ethical hacking and penetration testing [2][3] is an important feature of system protection and uses ethically driven attackers to perform attacks primarily with a view to finding vulnerabilities and their potential exploits. However, it does not typically assess the risk to victim systems in an attack, although may assess risk to target systems.

Other studies [4] aim at determining attack vectors to understand attacker behaviour by recognising that attackers have economic pressures (because they have financial limits) and potentially lack extensive target network information, so are resource-constrained. Whilst this recognises the uncertainty in the environment it does not address any form of RIDM.

Studies focusing on the derivation of "Secure State Estimation" in CPS [5][6] not only focus on system controller perspectives but also on attacker perspectives, because this is important information to both. However, whilst Secure State Estimation might feed into a risk assessment no studies focus on utilising RIDM by attackers on victim systems.

Despite the lack of research into RIDM by attackers on victim systems in typical cybersecurity related scenarios, the focus here is on performing relevant risk assessment for RIDM in EM cyberspace, so an extensive literature review was therefore performed on military-related EM Spectrum Operations (EMSO) involving the attack on enemy EM equipment targets using EM signals. There are three broad areas of EMSO [7]:

- **EM Warfare Support** (searching and detection of enemy EM signals)
- **EM Protection** (EM spectrum management to protect EM equipment)
- **EM Attack** (Offensive action – often called jamming – to degrade, disrupt or deny use of enemy EM equipment)

EM Attack uses transmitted signals from the attacker EM system aiming to degrade an enemy target system.

One differentiating feature of EMSO compared to cyber-attacks is that geophysical and meteorological complications can occur because the EM Topology of the physical environment can attenuate transmitted signals and this might reduce the consequences on victim or target systems. Nevertheless, such signal attenuation can be accounted for in calculations of received signal power at a victim/target, thereby still enabling determination of consequences.

An extensive literature search and review was performed to identify existing methods of Risk Assessment for EM Attack scenarios. The review identified that methods for calculating the likelihood (i.e. probability) that EM system degradation can be caused (in a generalised EM system for generalised transmitted signals) have been explored, for example by Genender et al [8], Peikert et al [9][10][11] and Li et al [12].

These research articles indicate that calculating probability needs to account for the stochastic nature of the variability of an EM-system functional properties. They use Monte Carlo methods and Fuzzy Set Theory to model the various potential failure modes using fuzzily defined statistical distributions to calculate victim system susceptibility.

III. Potential approach to RIDM

If risk can be quantified, an attacker can utilise a prior derived compatible quantified risk acceptability criterion to decide whether risk is acceptable. This is RIDM.

The derivation of appropriate risk acceptability criteria for the type of Quantified Risk Assessment Method (QRAM) needed for calculating victim risk and for performing RIDM in the complex, dynamic, uncertain environment addressed in this paper is an area requiring further work. A complication with such a study is that determination of risk acceptability criteria may however be somewhat subjective because it may depend upon personal characteristics. M'manga et al [13] describe the "*Risk Rationalisation Process*" which seeks to understand the rationale behind Risk-Based Decision-Making (RBDM) by utilising the "Observe Orient Decide Act" (OODA) model [14] [15] as a modelling baseline to design Personas [16] that are grounded in RBDM research. What this approach using OODA implies is that there is an element of personal perspective that may influence the derivation of appropriate risk acceptability criteria. That would need addressing in any further study.

However, other essential input to the RIDM process is quantified victim risk, based on the Kaplan and Garrick definition [17], which can be calculated using a QRAM with input from relevant methods that calculate probabilities of/and victim consequence metrics. These are discussed next.

In EM attacks, whilst it is probably impossible for an attacker to know the detailed component structure of a victim system (so no knowledge of any Fault Tree Analysis or Event Tree Analysis), it is potentially plausible to estimate a reasonable distribution of values of various high-level victim equipment properties by assuming that estimated victim equipment parameters are mean values of a statistical distribution of possible values. For EM Attack scenarios, the approach could adapt the method in Li et al [12], where threshold values are compared to a randomly sampled input signal. Adapting this approach, while accounting for the philosophy of Genender et al [8] and Peikert et al [9][10][11] (of calculating probability by randomly sampling fuzzily defined system parameters) an initial determination can be made as to whether the transmitted frequency can cause degradation by sampling the relevant minimum EM frequency parameter distribution to first check if the transmitted EM frequency affects the system. Having done that a similar approach can be used for checking signal power effects.

In summary: the literature reviewed indicates a QRAM involving randomly sampling from fuzzily defined distributions, to determine whether the received power and frequency are capable of causing some form of victim system degradation. Based on the number of random samples showing degradation then the probability of such consequences can be estimated. This is a Monte Carlo type approach based on assumed statistical distributions of parameters to model the fuzzy or uncertain victim equipment parameters.

IV. An applicable ontology

The dynamic nature of the environments described above indicate that real time data is essential to the QRAM. For example, structured data requirements could be defined via an EMSO-related baseline ontology. To investigate this, literature on Risk Assessment ontologies was reviewed first to determine both the status quo on current knowledge and an appropriate "Top Level Ontology" (TLO). This identified Sales et al [18] who created the "Common Ontology of Value and Risk" (COVER) using the TLO: Unified Formal Ontology (UFO) [19].

To create their ontology, Sales et al used the "Relational theory of risk" [20] where risk consists of a "risk object" plus an "object at risk" plus a "risk relationship" (connecting them). Fig. 2 shows the Risk Assessment part of COVER and shows "Risk Experience" is an important "Event" whereas an important "Relator" is "Experience Risk Assessment".

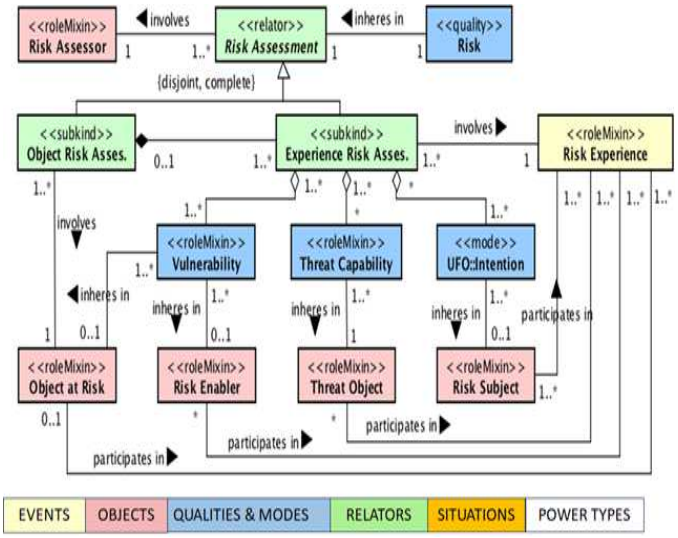

Figure 2: Risk Assessment part of COVER [18]

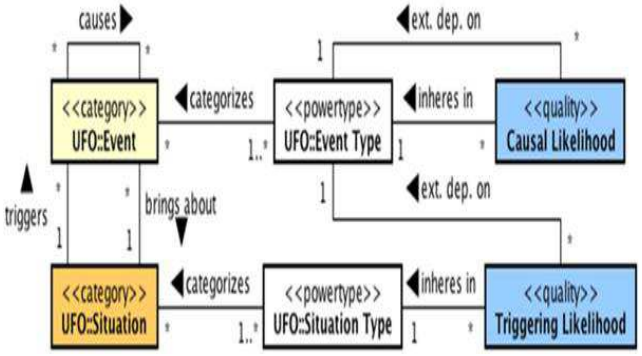

Figure 3: Representing Likelihood in UFO [18]

COVER can be extended to provide an applicable ontology by adding relevant victim system features that participate in defining the "Vulnerability" Quality, and that inhere in the "Object at Risk". It is worth noting here that Sales et al also illustrated how likelihood can be represented in UFO (Fig. 3).

V. MODELLING EM ATTACK SCENARIOS USING SYSTEM-OF-SYSTEMS THEORY

From the outset of this article the focus has been on how a conscientious attacker might determine the risk to victims. It was recognised that there is very little (if any) directly applicable literature that has considered this problem. The inference was drawn that methods for calculating EM Attack victim risk should utilise a QRAM and this will use methods for calculating the probability of specific consequence metrics. But perhaps there are additional aspects to feed into the risk assessment? To address this question, a method of modelling EM Attack scenarios would be helpful. An approach to this is to utilise SoS Theory to determine if modelling EM Attack scenarios is plausible and applicable.

Firstly, let's define a SoS. Maier [21] explains that a SoS contains elements:

"operating together to produce functions & fulfil purposes not produced or fulfilled by the elements alone"

So, SoS elements are operationally and managerially independent systems with independent useful purposes (i.e., not focused on a collective purpose) and typically geographically distributed with a configuration evolving over time and space.

SoS can be characterised into one (or sometimes more) of four models [22]:

- **Directed**: Centrally managed and built to fulfil specified purposes.
- **Acknowledged**: Designed by a designated (maybe self-designated) management with recognised objectives and resources (while constituent systems retain independence).
- **Collaborative**: No central management with elements collaborating voluntarily and independently.
- **Virtual**: No central management or purposes. Each element with limited views of other systems. Collaboration is possible only within these limitations.

The attacker, target and victim interactions can be illustrated using an SoS model. However, one of the features of an SoS is often referred to as "emergent behaviour". Dahmann [22] describes emergence as:

"*the objective of a SoS where multiple systems are brought together to generate capability which results from the interaction of the constituent systems. However, unanticipated, and undesirable emergent behaviour is a risk*"

So, before discussing "emergent behaviour" Dahmann indicates that it is important to understand "*the objective of a SoS".* In the present context, the purpose/mission of the SoS is to define the EM Attack scenario that enables the attacker to perform victim risk assessment. This is the perspective from which the emergent behaviour is to be judged (so not from a victim perspective, or an "interested onlooker", or anyone else). If it is judged from the Attacker perspective (as has been considered in this article) then one can argue that that promotes the Attacker to the role of a "designated manager". The phrase "manager" may not prima facia be obvious, but given emergence is observed from the Attacker perspective and the SoS objective is as described above, they are essentially *managing* the SoS. That is not to say the Attacker is fully controlling the SoS. Compare to a business

manager who is never fully in control because there are uncontrollable potentially random events like changes in weather and rational/irrational unknown decisions by people (in the current context these are victim system operators). Under these circumstances the only applicable SoS model is an Acknowledged SoS, therefore it is plausible to utilise SoS Theory for applicable modelling of EM Attack scenarios.

Within an Acknowledged SoS there are various direct/indirect interactions. Such interactions are similar to those found in ecological communities and a deeper examination of these indicates there are different types of direct/indirect interactions [23]. In the Acknowledged SoS (applicable to the contexts in this article) these interactions are "Human Interactions" (HI) where communication between people is performed (in whatever form) to gain information. This is not to say that communication will certainly occur, it is just to note that communication is a possibility. The motivation for such communication may be (for instance) to determine the level of trust between two people. Current methods and approaches in Human Factors are also inadequate in addressing SoS aspects associated with technical and organisational complexity [24]. However, in EM attacks there is unlikely to be communications between the attacker and the enemy system operator, but the option of communications with victims is not impossible. So, for a conscientious attacker designing risk controls, the option of multi-stakeholder (i.e., victims) communications and consultations (C&C) is available. Arguably, potential failure to perform C&C efficaciously, increases the probability of harms associated with:

- Dynamic evolution of the SoS (changing characteristics of victims).
- Changing interoperability needs related to individual victim systems.
- Compounding emergent behaviours within the SoS (i.e. new victim interactions).

This suggests, poor C&C potentially increases risk above risk-acceptability criteria, implying the probability (of high severity consequence in victim systems) is affected by how "good" C&C are between attacker and victim system owners. So, C&C is an essential risk control performed by the attacker. Measuring "goodness" of C&C requires further study.

VI. Conclusions

The paper has identified several significant and novel contributions. These form foundations for modelling conscientious attacking in EM cyberspace. They can be summarised as follows:

RIDM should be based on a Risk Assessment methodology accounting for fuzzy victim equipment parameters and the adoption of a Monte Carlo method to determine the probability (of degrading a victim system) and calculated for a consequence metric leading to quantified risk.

COVER can be extended to provide an applicable ontology for EM Attack scenarios by adding relevant victim system features that participate in defining the "Vulnerability" Quality, and that inhere in the "Object at Risk".

The only applicable SoS model applying to EM Attacks is an Acknowledged SoS indicating a common platform for applying models.

C&C between attacker and victim system owners are an important input to Risk Assessment probability calculations. Measuring "goodness" of C&C requires further study.

The study of appropriate risk acceptability criteria for the type of Quantified Risk Assessment described in this paper is also an area requiring further work.

To the best of the author's knowledge foundations for modelling conscientious attacking in EM cyberspace have never been addressed academically. These contributions therefore advance the state-of-the-art.

ACKNOWLEDGMENT

References

[1] Thompson, M., "Blurring the Lines: The Overlap Between Cyber and Electronic Warfare", *Journal of Electromagnetic Dominance, 25 October 2023*, [Online], 25 May 2024. Available: https://www.jedonline.com/2023/10/25/blurring-the-lines-the-overlap-between-cyber-and-electronic-warfare/

[2] D. Regalado, S. Harris, A. Harper, C. Eagle, J. Ness, B. Spasojevic, R. Linn and S. Sims, Gray Hat Hacking. 5th ed. New York: McGraw-Hill Education. 2018.

[3] M. Ceccato, P. Tonella, C. Basile, P. Falcarin, M. Torchiano, B. Coppens and B. De Sutter, "Understanding the behaviour of hackers while performing attack tasks in a professional setting and in a public challenge," *Empirical Software Engineering (EMSE),* vol. 24, issue 1, pp. 240-286, 2018.

[4] P.L. Bhattar, N.M. Pindoriya and A. Sharma, "False data injection in distribution system: Attacker's perspective," *International Journal of Critical Infrastructure Protection*, vol. 45, pp. 100672, 2024.

[5] Y. Shoukry, P. Nuzzo, A. Puggelli, A. L. Sangiovanni-Vincentelli, S. A. Seshia and P. Tabuada, "Secure State Estimation for Cyber-Physical Systems Under Sensor Attacks: A Satisfiability Modulo Theory Approach," *IEEE Transactions on Automatic Control*, vol. 62, issue 10, pp. 4917-4932, 2017.

[6] C. Zhang, X. Zhao, E. Tian and Y. Zou, "Stochastic important-data-based attack model and defense strategies for cyber-physical system: A data-

driven method," *International Journal of Robust and Nonlinear Control*, vol. 34 issue 8, pp. 5384 – 5398, 2024.

[7] Choi, S., Kwon, O.-J., Oh, H. & Shin, D., 2020. Method for effectiveness assessment of electronic warfare systems in cyberspace, Symmetry, 12(12), 1–16, 2107.

[8] E. Genender, H. Garbe and F. Sabath, "Probabilistic risk analysis technique of intentional electromagnetic interference at system level," *IEEE Transactions on Electromagnetic Compatibility,* vol. 56, issue 1, pp. 200–207, 2014.

[9] T. Peikert, H. Garbe and S. Potthast, "A fuzzy approach for IEMI risk analysis of IT-Systems with respect to transient disturbances," *IEEE International Symposium on Electromagnetic Compatibility*, pp. 1077–1082, 2015.

[10] T. Peikert, H. Garbe and S. Potthast, "Risk analysis with a fuzzy-logic approach of a complex installation," *Advances in Radio Science*, vol.14, pp. 91–96. 2016.

[11] T. Peikert, H. Garbe and S. Potthast, "Fuzzy-Based Risk Analysis for IT-Systems and Their Infrastructure," *IEEE Transactions on Electromagnetic Compatibility*, vol. 59, issue 4, pp. 1294–1301, 2017.

[12] K-J. Li, Y-Z. Xie, Y-H. Chen, Y. Zhou and Y-C. Hui, "Bayesian inference for susceptibility of electronics to transient electromagnetic disturbances with failure mechanism consideration," *IEEE Transactions on Electromagnetic Compatibility*, vol. 62, issue 5, pp. 1669-1677, 2020.

[13] A. M'manga, S. Faily, J. McAlaney, C. Williams, Y. Kadobayashi and D. Miyamoto, "Eliciting person characteristics for risk-based decision making," in *Proceedings of British HCI 2018*. Belfast, UK. 2018.

[14] J.R. Boyd, "A discourse on winning and losing," Maxwell Air Force Base, AL: Air University Library. Report Number M-U 43947, 1987.

[15] B. Brehmer, "The Dynamic OODA Loop: Amalgamating Boyd's OODA Loop and the Cybernetic Approach to Command and Control ASSESSMENT, TOOLS AND METRICS", in *10th International Command and Control Research and Technology Symposium. The Future of C2*, McLean, VA 13-16 June 2005. Homeland Security Digital Library: Command and Control Research Program (U.S.).

[16] R. F. Dam and T. Y. Siang, "Personas – A Simple Introduction" [Online]. Interaction Design Foundation. May 14 2024. Available: https://www.interaction-design.org/literature/article/personas-why-and-how-you-should-use-them

[17] S. Kaplan and B. J. Garrick, "On the quantitative definition of Risk," *Risk Analysis,* 1(1), pp 11-27, 1981.

[18] T.P. Sales, F. Baião, G. Guizzardi, J.P.A. Almeida, N. Guarino and J. Mylopoulos, "The Common Ontology of Value and Risk," in *Conceptual Modeling. ER 2018. Lecture Notes in Computer Science*, J. Trujillo, et al. Eds. Springer: Cham, 2018, 11157.

[19] Nemo, "UFO" [Online]. May 14 2024. Available: https://nemo.inf.ufes.br/en/projetos/ufo/

[20] Å. Boholm and H. Corvellec, "A relational theory of risk," *Journal of Risk Research,* vol. 14, issue 2, 2011.

[21] M. W. Maier, "Research challenges for Systems-of-Systems," *IEEE International Conference on Systems, Man and Cybernetics*, IEEE, vol. 4, pp. 3149–3154. 2005.

[22] J. S. Dahmann, "Systems of Systems Characterization and Types, (STO-EN-SCI-276) [Online]. 2015. Available: https://www.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-SCI-276/EN-SCI-276-01.pdf

[23] D. C. Moon, J. Moon and A. Keagy, "Direct and Indirect Interactions," *Nature Education Knowledge*, vol. 3, issue 10, pp. 50, 2010.

[24] Dogan, H., Pilfold, S.A. and Henshaw, M., 2011. The role of human factors in addressing systems of systems complexity. Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics, 1244-1249.

[25] The National Archives, "Open Government Licence for Public Sector Information" [Online]. July 16 2024. Available: http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3