Abstracts for Additional Presentations and Posters

at

The 11th European Conference on Cyber Warfare and Security

ECCWS 2024

A Conference

Hosted By

University of Jyväskylä and

JAMK University of Applied Sciences, Finland

27-28 June 2024

This booklet includes abstracts that correspond with presentations or posters submitted to the ECCWS conference without a paper publication. This is designed to be for reference to conference participants.

Contents

Polarisation Ideology in the Virtual Realm

Ferdinand J. Haberl, C. Lucian Reinfandt
DPI - Documentation Centre Political Islam, Vienna

ferdinand.haberl@dokumentationsstelle.at
lucian.reinfandt@dokumentationsstelle.at

Abstract: This contribution aims at illustrating that an ideology and its historic roots may have present implications on online radicalisation and extremism, on social media narratives as well as potential counter-narratives. In cyberspace identitarian Islamist movements (hereinafter: IIM) continue to foster an „us vs. them" narrative aiming to alienate the Muslim community and split society along ideological fault lines. This happens predominantly online but also occasionally transitions into the physical world. The resulting societal rifts have grave consequences for social cohesion and security. Indeed, those who may initially feel disenfranchised can ultimately, and at the last stage of radicalisation, opt for acts of violence or the jihad. This has unfortunately been observed many times over. However, the jihadi rationale behind such attacks are not necessarily always the actual atrocities on their own but the resulting divide and the elimination of a peaceful coexistence between religious groups in Europe and within Islam itself. In this regard both types of movements, jihadists as well as IIM, can use the vehicle of polarisation in order to influence a Muslim community finding itself in between religion and secularism. This polarisation as the jihadist ideologue Abu Bakr Naji assesses in his writings consists of those European Muslims who managed to find an individual balance between a spiritual identity and a broad and secular national context. According to the so-called Islamic State (hereinafter: IS) such moderate Muslims are to be isolated from Western societies. Some of them may then eventually be pushed into radicalisation through distrust and hostility from their fellow citizens because of terrorist attacks and propaganda. Furthermore, also Muslims opposing IS ideas thus become targets. However, is the core of this strategy unique to jihadist movements? Currently, very similar dynamics, with respect to the division of society by IIM can be observed, albeit here without calls for violence. It is true that one can hardly compare the online activities of an identitarian movement like the Muslim Brotherhood or the Hizb ut-Tahrir with a jihadist group. Still, one can certainly compare such polarising online narratives and investigate their origin in order to understand the implications the virtual world may have on the real one. We may thus find that by directly benefiting of the divisions deliberately created within society and through social media, IIM and jihadists have at least one thing very much in common: the elimination of the *gray zone* in the online and offline world.

Keywords: Online Narratives, Social Media, Ideology, Identitarian Movements, Jihad

Development of Curricula for Cybersecurity Degree Programs and Accreditation

Doug White and Russell Beauchemin
Roger Williams University, Bristol, USA

dwhite@rwu.edu
rbeauchemin@rwu.edu

Abstract: This presentation will be done by Doug White and Russell Beauchemin, two faculty from Roger Williams University Cybersecurity and Networking regarding the development of curricula related to the Cybersecurity industry and specifically related to accreditation. Roger Williams University obtained the National Security Administration [NSA] Accreditation and Center of Excellence Designation in 2022 and has been an undergraduate major since 2007. The presentation will include an overview of the NSA accreditation requirements and recommendations for institutions wishing to establish Cybersecurity degree programs which map to both the accreditation and the industry. Cyber Ranges, Virtual Environments, and selection of industry board members to optimize student outcomes are all components of this presentation.

Keywords Cybersecurity, Curricula, Cyber-Education, Cyber Accreditation

FICEC; Igniting Cyber Security Education and Partnerships in Central Finland

Arttu Laukkanen, Markus Takamaa and Antti Kariluoto
University of Jyväskylä, Jyväskylä, Finland

arttu.4.laukkanen@jyu.fi
markus.k.t.takamaa@jyu.fi
antti.j.e.kariluoto@jyu.fi

Abstract: The real-world changes in the geopolitical environment and the sheer number of internet-connected devices have raised the need for increased cybersecurity skills. Since modern information is stored in electric devices, the need for N know-how is evident whether it is an organisation, company, country, or individual. However, bringing the experts together with a united cause can sometimes take time due to the various needs, wants, and priorities of the organisations mentioned above.

In the Finnish cybersecurity landscape, Finnish organisations and institutions are constantly finding new ways to improve their cybersecurity. These ways include building expertise, researching and educating on cyber security, and supporting other institutions in achieving these. Central Finland is particularly known for this know-how; it houses various public, private, and educational facilities with cyber-security expertise.

Central Finland is the birthplace of the Finnish Center of Excellence in Cyber-security (FICEC). It brings all Finnish cybersecurity organisations together under one umbrella and strengthens them by managing common issues related to Skills, Education and cybersecurity research. FICEC was created by the University of Jyväskylä and JAMK University of Applied Sciences together and is currently

starting its operations as an organisation focusing on improving cyber-security in Finland. FICEC corroborates both universities' already matured partnerships in cyber security.

FICEC aims to improve cyber security in Education and Research while also Influencing discussion related to cybersecurity topics. This improvement is made, for example, by coordinating Cybersecurity education management in Finnish Higher education facilities and creating consortiums for related research projects. FICEC also promotes new research innovations in cybersecurity while influencing public spending on improving cybersecurity resilience. FICEC's vision, in the long run, is to become one of the leading international research and education centres and become Finland's leading focus point of cyber-security education. With the coordination of FICEC, the Finnish cyber-security organisations have become more than the sum of our parts.

Keywords cyber security, education, research, resilience

Non-military Drones Jeopardizing National Security– Starvation as a Weapon of War.

Claris Diaz and Emilian Kavalski
Jagiellonian University, Krakow, Poland

clarismd3@gmail.com
emilian.kavalski@uj.edu.pl

Abstract: Food security is climbing up the security agenda of both states and international organizations. The projections are that by 2050 much of the global population will face severe food insecurity. From now until this unprecedented time, any nation with the means to assure food security for other nations will have leverage. Diverse forms of Smart Agriculture have been suggested as relevant modes of addressing such security threats. Yet, can the very technologies that are being deployed to enhance food security become the sources of new security threats? The paper looks at the use of drones for precision agriculture. In particular, the China-based drone manufacturers XAG and DJI have come to dominate the global smart agriculture marketplace. Their drones are distributed in the world's top wheat and rice-producing countries such as the United States, Thailand, and Vietnam. Aside from having geospatial intelligence about farms and fields, drones can also track crop health and yield, detect crop disease, and collect critical data such as soil conditions. This information can be taken to manufacture seeds or fertilizers that ensure healthy and abundant crops, creating market dependency. This knowledge can also facilitate the creation of crop-specific diseases, such as Wheat smut, which was used as a bioweapon to destroy Iran's cereal crops during the Iran-Iraq war. The paper explores the potential weaponization of such technologies by looking at how data gathered by these drones can be used for direct or indirect (and hybrid) attacks on strategic infrastructures and supply chains. Food insecurity in any nation-state can lead to financial crises, political instability, and conflict. The convention is that the awareness of how non-military drones, specifically those used in Smart Agriculture, can be used to jeopardize national security may assist the consideration of relevant actions to circumvent such threats while enhancing both national and global food security.

Keywords drones, precision agriculture, food security, food infrastructure

Quantum- and cyber-secure smart devices for use in the smart Metaverse networks

Aarne Hummelholm
University of Jyväskylä, Finland

aarne.hummelholm@elisanet.fi

Abstract: Cyber security threats in our societies have expanded with the increasing digitization of services, virtualization and slicing of communication networks. Mobile network technologies are moving from 5G to 6G. The edge devices of telecommunication networks are also changing and must adapt to these new requirements based on technical development. Metaverse environments are also coming into use. In these new service environments, we use artificial intelligence (AI) solutions in service development, development of technical solutions, optimization of service quality and threat analysis. Virtual reality solutions are also used in these environments. These new technical development solutions for networks and services provide many opportunities for cyber attackers, hackers, and various government actors to attack, manipulate and decentralize our systems and services anywhere and anytime around the world.

That's why we need new types of smart devices and new requirements for them, as well as new quantum encryption systems for using in wireless networks, so that the devices can work safely in these really challenging environments. These smart devices can also work independently without connecting to other networks. They can act as an active part of the PAN network (Personal Area Network) and collect sensor data and information from the PAN network area and send information to edge and connection networks. These new smart devices can form small cellular networks with each other without connecting to other networks and communicate with each other in a device-to-device format. Authorized users can join and leave this mobile network depending on the situation. This new type of smart terminal can meet the quality challenges of new services in 5G and 6G networks.

The most critical planned aspects are the reliability, real-time and transfer time delays of the services used. In this research project, we are also developing quantum encryption technology. Quantum cryptography gives users confidentiality, trust, and privacy protection to use our smart services in our future smart societies and its metaverse world.

Keywords smart device, cyber threat, artificial intelligence (AI), quantum encryption, metaverse.

Cybersecurity Framework and Application Process for the Health Sector

José Martins[1] and Alberto Caria[2]
[1]Palconsulting, Lisbon, Portugal
[2]Paldata, Portugal

jose.martins@palconsulting.pt
alberto.caria@paldata.pt

Abstract: This article presents the HISC4ALL project under development, whose main objective is to design an Information Security and Cybersecurity Framework developed for the healthcare sector in Portugal, based on a research and development project funded by the European Union [1].

This framework for Information Security and Cybersecurity controls is aimed at the health sector and is incorporated into a web application, which aims to answer the following research question: - How can we guarantee the confidentiality, integrity, availability, non-repudiation and authenticity of data/clinical information shared between healthcare entities to minimise Information Security and Cybersecurity risks?

In addition to the literature review, two case studies will be carried out, one at the National Institute of Medical Emergency and the other at the University Hospital Centre of São João (Portugal). Modelling of attacks on critical medical devices will also be carried out. This will make it possible to understand the reality of how organisations in the health sector operate and to obtain relevant input for the design, which will be validated by two panels of experts, one of whom is from the health sector.

The main results of this phase of the research are presented in this article: (i) the conceptual model of the framework; (ii) the main categories of security controls for each security dimension; (iii) the web application interface; (iv) the general application method.

The growing digital transformation in the health sector brings numerous advantages, but at the same time, there is also an increase and growing sophistication of cyberattacks. As a result, the fundamental properties of Information Security and Cybersecurity, i.e. confidentiality, integrity and availability and, in the particular case of healthcare, non-repudiation and authenticity, must be permanently guaranteed.

This project is expected to contribute to Information Security and Cybersecurity in the health sector in Portugal and beyond, by providing a framework of controls and a web application that facilitates their application.

[1] Funded by the European Union, under a grant agreement Nº 101100701.

Keywords Cybersecurity and Information Security Framework, Cybersecurity for the Health Sector, Cybersecurity Governance and Management

Enabling Military Cyber Warfare Exercises and Testbeds with Open-Source Software

Christopher May and Jeff Mattson
Carnegie Mellon University, Pittsburgh, Pennsylvania, USA

cjm@sei.cmu.edu
jmattson@sei.cmu.edu

Abstract: The United States military and other government agencies utilize exercises, competitions, simulations, and testbeds to great effect in developing and evaluating its cyber warriors as well as testing new tactics & capabilities. New policies have recently permitted the release of these cutting-edge technologies as open-source software. This talk will showcase many of these platforms and simulation tools developed for the US Government and discuss how anyone can now leverage them to improve their cyber mission readiness. Demonstrations and examples of unclassified US government implementations will be used to facilitate broader adoption of these capabilities.

Carnegie Mellon University's Software Engineering Institute (SEI) is a US Department of Defense research and development center and has supported the US military for 40 years. Christopher May leads SEI's Cyber Mission Readiness group and has created exercise and testing solutions for the US Department of Defense for 30 years. He also taught applied cybersecurity courses in CMU's master's of science in information security program for 17 years.

Keywords Range, Testbed, Open-source, Simulation, Exercises

Practical Use of AI for Cybersecurity

Camden Hackett
Roger Williams University, Bristol, USA

chackett339@g.rwu.edu

Abstract: The heart of the presentation explores diverse applications of AI in cybersecurity. From Darktrace's real-time threat detection using unsupervised learning to Exabeam's behavioral analytics combating insider threats, and Cylance's AI-based proactive threat prevention, the examples span network security, phishing detection, incident response automation, user authentication, vulnerability management, deception technology, and cloud security. Each instance illuminates how AI is reshaping fundamental aspects of cybersecurity. The presentation underscores improved threat detection accuracy, accelerated response times, task automation, and heightened defense against evolving threats. However, challenges, including potential biases in AI models, and ethical considerations are acknowledged, emphasizing the importance of maintaining ethical standards in the cybersecurity realm.

Keywords Endpoint Security, Phishing Detection, User Authentication, Incident Response

Tracking and Mitigating "Dirty" Data in Containers

John S Hurley,
National Intelligence University, Bethesda, USA

john.s.hurley@odni.gov

Abstract: Containers are considered such an essential asset in data sharing because application codes can be packaged with their libraries and dependencies. As a result, the code can be run in a variety of different environments including cloud, on prem, and edge locations. Containers are also valuable due to the greater focus on protecting and distributing data and running applications. One of the most popular containerization platforms is Docker, actually a Platform-as-a-Service (PaaS) offering in high demand largely because of its flexibility. Docker has the ability to take almost any application with its associated dependencies and transform it into a virtual container which can be run on a variety of different operating systems. Unfortunately, a variety of different factors can contribute to container breaches, including bad actor cloning; codebase changes, commits, and pull requests; third-party access; improper scanning; and container vulnerabilities. Many of the solutions that exist are directed to new data being entered into the containers. However, very little work has been devoted to dealing with the “dirty” data, i.e., breached data already in containers, that continue to be transported and exchanged between systems and locations. In this effort, the focus is on ways to track and mitigate “dirty” data using machine learning techniques. The study emphasizes and is limited to the breaches due to software components not interacting with package managers. The effort shows that it is critical to account for the history of data in its lineage from when and how the data is created to the different locations and processes used in addressing the data. Ensemble learning methods are then used to show how the different attributes and dependencies of the application can impact the likelihood that “dirty” data makes it into the containers.

Keywords Containers, Interactions, Application, Package Manager, Software Components,

Hitler Youth, Denazification, Education, Ethics, Anticipatory Ethics

Richard Wilson
Towson University, Towson, USA

wilson@towson.edu

Abstract: The Hitler Youth was the youth organisation of the Nazi Party in Germany. Its origins date back to 1922 and it received the name Hitler-Jugend, Bund deutscher Arbeiterjugend ("Hitler Youth, League of German Worker Youth") in July 1926. From 1936 until 1945, it was the sole official boys' youth organisation in Germany and it was partially a paramilitary organisation. It was composed of the Hitler Youth proper for male youths aged 14 to 18, and the German Youngsters in the Hitler Youth (Deutsches Jungvolk in der Hitler Jugend or "DJ", also "DJV") for younger boys aged 10 to 14.

Russian textbooks praising Vladimir Putin’s invasion of Ukraine are an attempt to encourage “self-sacrifice” among schoolchildren, experts have warned. In September, Russia rolled out new history

textbooks to schools that claim Ukraine is an “ultranationalist state” being used as a “battering ram” by the United States to “destroy Russia”.

One chapter claims that Ukrainian membership of Nato could have led to a catastrophic war and “possibly the end of civilisation”, an outcome it says Russia had to prevent. Putin's claim of fighting against Ukraine 'neo-Nazis' distorts history and a more accurate account of Putin’s and using techniques similar to those used to develop the Hitler youth place Putin squarely in the camp of Neo-Nazi’s not Ukraine.

This analysis will focus on the Ethical and Anticipatory Ethical issues related to the Russian information war on and effort to destroy Ukrainian Culture through the use of propaganda techniques used to influence the Hitler but now applied to Ukraine/Russia War and by extension to the recent US attack in a number of states on education.

Keywords Hitler Youth, Denazification, Education, Ethics, Anticipatory Ethics

The Denial of Science, Disinformation and Anti Vaxxers: An Ethical and Anticipatory Ethical Analysis

Richard Wilson
Towson University, Towson, USA

wilson@towson.edu

Abstract: The same tactics used to cast doubt on the dangers of smoking and climate change are now being used to downplay COVID. In 2020, there was a historic level of disregard of scientific advice with respect to the COVID-19 virus, a disregard that made the pandemic worse in the U.S. than in many other countries. But while the events of 2020 may feel unprecedented, the social pattern of rejecting scientific evidence did not suddenly appear this year. There was never any good scientific reason for rejecting the expert advice on COVID, just as there has never been any good scientific reason for doubting that humans evolved, that vaccines save lives, and that greenhouse gases are driving disruptive climate change. To understand the social pattern of rejecting scientific findings and expert advice, we need to look at the promotion of disinformation have roots in the history of tobacco.

Throughout the first half of the 20th century, most Americans saw science as something that made our lives better. Science had deepened our understanding of the natural world, which helped us to cure diseases, light our homes and bring new forms of entertainment into our lives. corporate R&D really did produce products that measurably improved many American lives. But corporate America was also developing the playbook for science denial and disinformation.

The chief culprit science denial was the tobacco industry, whose playbook has been well documented by historians of science, technology and medicine. It disparaged science by promoting the idea that the link between tobacco use and lung cancer and other diseases was uncertain or incomplete and that the attempt to regulate it was a threat to American freedom. The industry made products more addictive by increasing their nicotine content while publicly denying that nicotine was addictive. With these tactics, the industry was able to delay effective measures to discourage smoking long after the scientific evidence of its harms was clear.

This analysis will focus on the Ethical and Anticipatory Ethical issues related to the influence The Denial of Science and Disinformation on the information warfare conducted by Anti Vaxxers.

Keywords Denial, Science, Disinformation, Anti -Vaxxers, Ethics, Anticipatory Ethics