

Cyberwatch

FINLAND

Special media of strategic cyber security

MAGAZINE 2019/6

DRONE CONGRESS AND SEMINARS
**SPECIAL
EDITION**
CYBER SECURITY NORDIC

TRUST IS THE
CORNERSTONE OF
CYBER SECURITY

THE 1ST DRONE CONGRESS IN HELSINKI

1-3 OCT, 2019
+ CYBER SECURITY NORDIC 2-3 OCT, 2019

Aeronautics Group

DRONE CYBER
EVENT

Cyberwatch
Finland



Drones in cyber
security environment

Contents

2019/6

3	Editorial
4	Drones in cyber security environment
14	Drone congress
22	Cyber Security Nordic
26	Aeronautics: A head of its time
30	Autonomous and secure drone swarming - what is needed?
36	GOF U-space project demonstrates the future of Drone Traffic Management in Finland and Estonia during 2019
42	Cyberwatch review
48	Sensor on the edge
51	VTT drone accelerator program
52	What is wrong with legacy IP security tools?
55	Helsinki-East Aerodrome - where the future of aviation takes flight
56	Protecting water utility against nation state cyber adversary
59	Lessons learned from Ultrahack's Drone Tournament
60	Disinformation threatens democratic processes, but potentially also your business
66	Simplifying IoT connectivity

Cyberwatch

MAGAZINE

Special media of strategic cyber security

Publisher
Cyberwatch Finland Oy
Eteläranta 10
00130 Helsinki
Finland
www.cyberwatchfinland.fi

Producer and commercial cooperation
Pertti Jalasvirta
pertti@cyberwatchfinland.fi

Layout
Atte Kalke, Vitale Ay
atte@vitale.fi

ISSN 2490-0753 (print)
ISSN 2490-0761 (web)

Print house
Printall, Tallin



Cyber security challenge of UAV:s and the importance of education

WE ARE LIVING in an era where drones and cyber security are the drivers of the future societies. We are looking for new ways to use drones as a part of our every day life without forgetting security and privacy.

New cyber security tools are currently being researched and are soon at our disposal. The hardware, software and methodological system forms a whole that will help us manage the evolving strategic cyber security challengers

The key to success is having better strategic situational awareness. New solutions and tools can be the game changers, when we are changing the threat of cyberspace to an opportunity.

The need for automated, scalable, machine-speed vulnerability detection and patching is extensive and increasing rapidly. Today, the process of finding and countering bugs, hacks, and other cyber infection vectors is still effectively artisanal. Professional bug hunters, security coders, and other security processes are working 24/7 searching millions of lines of code to find and fix vulnerabilities.

Rushing to develop applications of drone technology without understanding the complex security risks can result to many complicated challenges for which we are not prepared. It is crucial to understand the risks associated with the drones or unmanned aerial vehicles (UAV).

It is important to remember that in the design of all new products and solutions, cybersecurity must be a part of its foundation. It will be more complicated and costly to fix the security challenges, protect weak systems and processes against attackers. It will also be much cheaper to incorporate cybersecurity thinking into the design from the start, because repairing it will be expensive later on. The goal must therefore always be to produce a cyber-safe product or solution. We should not give the cyber criminals too much of an advantage by designing less secure products.

EDUCATION PLAYS A VITAL ROLE IN THE CONSTANTLY EVOLVING CYBER WORLD

It has been proven that employees who feel taken care of and acknowledged by their employers are more committed to the success of the company. They work harder and gain much better results especially in the long run. By investing in building the capacity of the cyber security of labor, you invest in the future success of your organization. Education is the best and most cost-effective way to improve the resilience of your company or organization.

The benefits of lifelong cyber security learning go beyond career advancement.

It can help you to understand how the cyber security world works. It can help you realize your passion and boost your creativity. The It goes without saying that learning about cyber challenges is a never-ending process. The cyber world is rapidly changing, thus people need lifelong learning to advance their skills and stay updated.

Don't be an easy target - build competency! |

Pertti Jalasvirta,
Cyberwatch Finland partner, President of Finland Chapter of World UAV Federation (WUAVF)



Editorial

Trust is The Cornerstone of Cyber Security

TRUST OR LACK OF TRUST is becoming the key success factor for cybersecurity. The entire ecosystem needs to be taken into account when building cyber security - a zero trust mindset is becoming a new megatrend in the operations of both the governments and cyber companies. The cyber security of your own organization or company is no longer enough, you have to consider the entire ecosystem or operating environment. The ever evolving cyber espionage is constantly looking for vulnerabilities and weak points in people, in processes and ways of working as well as technology. Keeping your own data secure is not enough for your own protection; you must take into consideration the level of protection of your partner, your customers, and your stakeholders. In particular, the outsourcing of cybersecurity services needs to be more precise. It is difficult to restore lost confidence - almost impossible in the cyber world. The consequences can be catastrophic, especially in business - leadership based on foresight and proper situational awareness must be emphasised - Even the best technology is not enough to compensate the human error.

Zero trust is a cybersecurity strategy that embeds security throughout the architecture for the purpose of stopping data breaches. This data-centric security model eliminates the idea of trusted or untrusted networks, devices, personas, or processes. Implementing zero trust requires rethinking how we utilize existing infrastructure to implement 'security by design' in a simpler and more efficient way.

The development of drones has been fast and rather inter-dimensional. The starting point has been military requisites, but the explosive growth in recreational use has led to a fall in prices and rapid technological development. At the same time, it has been seen that drones are useful for many civilian needs, such as surveillance tasks, various logistical transport tasks, agricultural purposes, etc. It would probably be better to talk about self-propelled devices, since some of these tools do not fly but crawl, swim or dig.

These self-guided digital tools are becoming part of the critical infrastructure of modern societies, thus naturally becoming targets of cyber attacks. For example, their control systems are easily intercepted, disrupted, and/or deceived by cyberattacks. In many cases the principle of "security by design" has been forgotten. Security precautions are only considered when a realization is made on the extent of change and how fast the capability of the modern self-propelled devices is increasing.

The shutdown of Gatwick Airport, in December 2018, was the first serious warning of the kinetic threat posed by drones. It is a reminder of the need for regulation and the inability of the security authorities to deal with these new threats. Drones have also been developed as a platform for cyber attacks. They can be used to conduct aggressive cyber intelligence, influence and deception. No need to drive a vehicle near a target anymore, but the operation can be handled with smart small drones or with a swarm of drones. The users appear to be state actors as well as cybercriminals and various activist groups. This development is again a reminder of how useful digital innovations can be misused and create new security threats.

In the future, we will certainly see new "drone operations" as a part of the growing hybrid influencing. The development of self-propelled devices must be taken seriously in future cyber security development projects, as both a threat and an opportunity. Military use is also increasing and evolving as a part of the development process for civilian use. The June conflict between Iran and the US is a living example of the importance of cyberattacks and drones as a part of military operations. |

Aapo Cederberg
Managing Director, Cyberwatch Finland
Chairman of Cyber Security Committee of World UAV Federation (WUAVF)



Drones in cyber security environment

text: Prof. Martti Lehto
University of Jyväskylä



ABSTRACT

➤ Aerial unmanned vehicles (AUV) are currently used for a wide range of operations such as border surveillance, surveillance, reconnaissance, transport, aerial photography, traffic control, earth observation, communications, broadcasting and armed attacks. AUVs are presumed to be reliable, automated and autonomous machines, providing their services at any time and everywhere.

AUVs are extremely suitable for long missions that strain flight crews or put them in harm's way. Two advantages can be gained by eliminating the flight crew: 1) performance improves (range, endurance, increased payload and maneuverability, smaller physical size and lower observability) and; 2) the ability to take higher risks.

UAV/RPAS/drone cyber security has largely focused on exploitable vulnerabilities in either the communication channels or the hardware/software stack on the vehicle. Such attacks have focused on exploiting unencrypted communication over wireless media to implement eavesdropping, cross-layer attacks, signal jamming, denial of

service, and dropping Wi-Fi communication with ground control. Other attacks on drones involve GPS (Global Positioning System) spoofing attacks to fool the drone into moving to a different destination (possibly with the intention of hijacking the drone).

In the same time UAV or drone can be a cyber attack platform. Specially equipped drone can track signals based on Wi-Fi, radio frequency identification (RFID) and the Bluetooth and 802.15 specifications (PAN/WPAN communication). Combined with a GPS capability drone correlates signals to the location where they're detected. So, the drone spy not only on phones, tablets, and computers, but also, potentially, on pacemakers, fitness bracelets, smartcards, and other electronics. Additionally, drone can function as visual tracking platforms even without the use of beacons or GPS.

Swarms of small drones could soon become an important part of the modern military arsenal. The swarm idea inherently drives drones towards autonomy which allows many different kinetic and non-kinetic operations.

INTRODUCTION

➤ There is no one standard when it comes to the classification of unmanned aircraft system (UAS). Defense agencies have their own standard, and civilians have their own categories for UAS. UAVs can be roughly divided into fixed wings and rotary wings. Other classification argument is size, Maximum Gross Takeoff Weight (MGTW), range and endurance. For combat is two main groups: Unmanned Combat Aerial Vehicle (UCAV) and, Unmanned Combat Aerial Rotorcraft (UCAR). These can be categorized by performance and combat mission.

According U.S. DoD an UAS is a "system whose components include the necessary equipment, network, and personnel to control an unmanned aircraft." UAV is the acronym of Unmanned Aerial Vehicle.

The International Civil Aviation Organization (ICAO) employs the acronym RPAS (Remotely Piloted Aircraft System). The definition associated is that these systems as "based on cutting-edge developments in aerospace technologies, offering advancements which are opening new and enhanced civil-commercial applications as well as improvements to the safety and efficiency of the entire civil aviation."

French Directorate for Civil Aviation (DGAC) see commercial unmanned aerial vehicles as a drone. In a general way, in French speaking countries are mainly using this drone term. For many UAV is mostly used in a military context, so drone cover both civil and military purpose any type of aerial unmanned vehicle.

This article uses the term drone to cover the whole spectrum of aerial unmanned vehicle.

” This article uses the term drone to cover the whole spectrum of aerial unmanned vehicle.

1. DRONE AND ITS SUBSYSTEMS

1.1 DRONE SUBSYSTEMS

Manned and unmanned aircraft of the same type generally have recognizably similar physical components. The main exceptions are the cockpit and environmental control system or life support systems. Drones carry often different type of payloads (such as a camera). Some of the drones can carry heavy payloads like weapons and other armaments. Drone-system may divide following five subsystems:

1. THE HUMAN ELEMENT consists of the drone pilot and the possible payload operator, if necessary. Drone personnel also include maintainers, mission commanders and intelligence analysts. At the ground station, drone is operated remotely by a team of two: a pilot and a sensor/payload operator. The pilot's primary function is flying the plane, while the sensor operator monitors the performance of the many different sensor systems utilized by the drone. Payload operator uses the possible armament of the drone. The increase in autonomy in drones reduces and changes the role of human in operations.

2. THE CONTROL ELEMENT handles multiple aspects of the mission, such as Command and Control (C2), mission planning, payload control and communications. It can be ground-based, sea-based or airborne. The portion of the Control Element where the drone pilot and the payload operator are physically located is referred to as the Ground Control Station (GCS). Here too, autonomy is reduced the human activity.

3. DATA LINKS include all means of communication among the drone, the Control Element and every relay station and network node in-between them. They are used for any means of data transfer. Data and Control link functions are:

- Uplink from the ground station or a satellite to send control data to the drone.
- Downlink from the drone to send data from the onboard sensors and telemetry system to the ground station.

4. THE SUPPORT ELEMENT includes all the prerequisite equipment to deploy, transport, maintain, launch and recover the drone and enable communications. These tasks are typically conducted by Launch and Recovery Units (LRU).

5. THE PAYLOAD includes sensors (camera, laser pointer, IR-camera etc.), communication equipment, weapons or cargo. They are carried either internally or externally by the drone.

1.2 DRONE AUTONOMY

The autonomy allows reducing the frequency at which the operators must interact with the drone supporting the implementation of more robust system solutions, where the role of the operators is to manage and supervise, through appropriate human machine interface, the command and control functions without direct interaction.

There are various ways to discuss autonomy in weapon systems. According Maj Thomas Payne USAF (2017) although precise definitions are critical for design and engineering purposes, understanding the debate about autonomy requires an acknowledgment of these differing uses of the term, typically centered on ethically relevant subprocesses of the system as a whole; targeting, goal-seeking, and the initiation of lethality.

According US DoD (2018) autonomy is defined as the ability of an entity to independently develop and select among different courses of action to achieve goals based on the entity's knowledge and understanding of the world, itself, and the situation. Autonomous systems are governed by broad rules that allow the system to deviate from the baseline. This contrasts with automated systems, which are governed by prescriptive rules that allow for no deviations. While early robots generally only exhibited automated capabilities, advances in Artificial Intelligence (AI) and Machine Learning (ML) technology allow systems with greater levels of autonomous capabilities to be developed. The future of unmanned systems will stretch across the broad spectrum of autonomy, from remote controlled and automated systems to near fully autonomous.

Autonomous categories are:

- **Human-in-the-loop:** In this mode, humans retain control of selected functions preventing actions by the AI without authorization; humans are integral to the system's control loop.
- **Human-on-the-loop:** The AI controls all aspects of its operations, but humans monitor the operations and can intervene when, and if, necessary.
- **Human-out-of-the-loop:** The AI-algorithms control all aspects of system operation without human guidance or intervention. The autonomous drone engages without direct human authorization or notification.

Autonomy results from delegation of a decision to an authorized entity to act within specific boundaries. An important distinction is that systems governed by prescriptive rules that permit no deviations are automated, but they are not autonomous. US Office of the Under Secretary of Defense (2016) addresses that to be autonomous, a system must have the capability to independently compose and select among different courses of action to accomplish goals based on its knowledge and understanding of the world, itself, and the situation.

2. DRONE'S MILITARY AND CIVILIAN OPERATIONS

2.1 MILITARY OPERATIONS

The development of unmanned aerial vehicles is intensifying as technology becomes cheaper. Drones can be used in a flexible manner in different tasks such as intelligence, surveillance, target acquisition, and recognition missions, in strikes against surface targets, over-the-horizon relaying of information, Electronic Warfare (EW), Combat Search and Rescue (CSAR), Chemical, Biological, Radiological and Nuclear Warfare (CBRN), logistic replenishments and Counter Improvised Explosive Devices (C-IED) in a favorable environment or in areas where the risk level is elevated.

Drones are presumed to provide their services at any time, be reliable, automated and autonomous. Based on these presumptions, governmental and military leaders expect drones to improve national security through surveillance or combat missions. To fulfill their missions, drones need to collect and process data. Therefore, drones may store a wide range of information from troop movements to environmental data and strategic operations. The amount and kind of information enclosed make drones an extremely interesting target for espionage and endangers drones of theft, manipulation and attacks.

Various types of air domination systems are being considered to enable a military force to dominate an area from the air for extended periods and deny enemy movements and maneuvering. The unmanned combat aircraft can be divided into two categories according to their operating model: loitering or swarming.

In USA current systems under consideration are standard weaponized drones or small expendable loitering weapons, fitted with imaging sensors, such as the Low-Cost Autonomous Attack System (LOCAAS). Operating in swarms of "intelligent munitions" weapons, the LOCAAS can autonomously search for and destroy critical targets while aiming over a wide combat area.

A loitering weaponized drone (also known as a suicide drone or kamikaze drone) is a weapon system category in which the weaponized drone or munitions loiters around the target area for some time, searches for targets, and attacks once a target is located. Loitering systems enable faster reaction times against concealed or hidden targets that emerge for short periods without placing high-value platforms close to the target area and allow more selective targeting as the actual attack mission can be aborted.

2.2 CIVILIAN OPERATIONS

Various UAVs are increasingly being used for various civilian purposes, such as government missions (law enforcement, border security, coastguard), firefighting, surveillance of oil and gas industry infrastructure and electricity grids/ distribution networks, traffic control, disaster management, agriculture, forestry and fisheries, earth observation and remote sensing and communications and broadcasting. In 2016, PwC estimated the value added of the drone economy at \$ 127 billion. According SESAR (Single European Sky ATM Research) the growing drone marketplace shows significant potential, with European demand suggestive of a valuation in excess of EUR 10 billion annually, in nominal terms, by 2035 and over EUR 15 billion annually by 2050.

The development of the civil drone industry is dependent on the ability of drones to operate in various areas of the airspace, especially at very low levels. In aggregate, some 7 million consumer leisure drones are expected to be operating across Europe and a fleet of 400 000 is expected to be used for commercial and government missions in 2050.

Critical infrastructure (CI) includes large variety elements from nuclear reactors, chemical facilities, water systems, logistics and airports to healthcare and communications, and now drones are growing a very important part in this critical infrastructure environment. They have numerous tasks in critical infrastructure maintenance and protection. Human work is reduced, and tasks can be performed cost-effectively.

At the same time CI must deal with the new and emerging threat of drones. The most headline-grabbing risks tend to be those of physical and electronic attacks. For example, drones could carry explosives into a nuclear power plant or get close enough to execute cyber-attacks, causing disruptions or even mechanical failures or even stealing sensitive data. The low-cost, global proliferation and capabilities of drones weighing less than 20 pounds make them worthy of specific focus. Future adversaries could use these small systems to play havoc with critical infrastructure both in the air and on the ground, necessitating new actions to defend CI assets. Today several small UASs have payload capacity, extended range, and the ability to be GPS- or pilot-guided to locations with great precision.

3. DRONE SWARMING

➤ Drones are currently in widespread use around the world, but the ability to employ a swarm of these systems to operate collaboratively to achieve a common goal will be of great benefit to national defence. A swarm could support lower operating costs, greater system efficiency as well as increased resilience in many areas.

Zachary Kallenborn (2018) from US National Defense University defines drone swarm technology as the ability of drones to autonomously make decisions based on shared information. This has the potential to revolutionize the dynamics of conflict. In fact, swarms will have significant applications to almost every area of national and homeland security. Swarms of drones could search the oceans for adversary submarines. Drones could disperse over large areas to identify and eliminate hostile surface-to-air missiles and other air defenses. Drone swarms could potentially even serve as novel missile defenses, blocking incoming hypersonic missiles. On the homeland security front, security swarms equipped with chemical, biological, radiological, and nuclear (CBRN) detectors, facial recognition, anti-drone weapons, and other capabilities offer defenses against a range of threats.

McMullan (2019) argues that swarming drones come in different shapes and sizes. The DARPA, for example, has been working on a program dubbed Gremlins; micro-drones the size and shape of missiles, designed to be dropped from planes and perform reconnaissance over vast areas. On the

other side of the spectrum is the larger XQ-58 Valkyrie drone, measuring almost 9m in length. It has been called a 'loyal wingman' for a human pilot - able to carry precision-guided bombs and surveillance equipment. It recently completed its first successful test flight, although the eventual aim is for it to work in a group alongside a manned fighter jet. In either case, the biggest advantage of a 'swarm' is the ability of machines to work together in numbers.

Finland's MoD (2015) addresses that in some cases, drones can carry out missions better and cheaper than manned aircraft. The widespread proliferation of Micro Air Vehicles (MAV) which are difficult to detect is on the cusp of becoming extremely challenging for air defences. Even the smallest drones are suitable for intelligence and PGM target designation. Moreover, they can double as weapons, even inside buildings. The most radical concepts focus on replacing the intelligence-targeting-fire chain; they aim at achieving a rapid weapons effect with the coordinated use of swarming unmanned aerial vehicles. This requires sufficient survivability and cost-effectiveness from drones in order to saturate the defence.

Haberl and Huemer (2019) described in their conference paper the drone swarm attack. In 2018 the Russian Ministry of Defence announced that 13 drones, which had been fitted with small bombs managed to attack Russian bases in Syria. Such drones, which are intended to explode on impact need to be modified in order to carry explosives and it is easy to imagine how 3D-printing could come in handy in this regard, especially since drones are capable of evading missile warning systems without any additionally needed infrastructure or equipment.

4. CYBER THREATS AGAINST DRONES

➤ **4.1 CYBER VULNERABILITIES**
According Hartmann and Steup (2013) drones are highly dependent on wireless systems and therefore can face considerable cybersecurity risk. Drone security has largely focused on exploitable vulnerabilities in either the communication channels or the hardware/software stack on the drone. Such attacks have focused on exploiting unencrypted communication over wireless media to implement eavesdropping, cross-layer attacks, signal jamming, denial of service, and dropping Wi-Fi communication with ground control, to name a few. Other attacks on drones involve GPS spoofing attacks to fool the drone into moving to a different destination (possibly with the intention of hijacking the drone).

Hartmann and Steup continue that the vulnerability may impose a threat to the systems security. Interestingly, attackers searching for targets go the same way as system architects designing a secure system. An attacker is searching for a system vulnerability imposing a high threat, implying a high risk. A system architect is trying to eliminate vulnerabilities imposing high threats and hardens the system through the integration of coping mechanisms. To heighten the systems security, it is essential that the system designer finds vulnerabilities before attackers do.

4.2 CYBER-ATTACK VECTORS

US Joint Air Power Competence Centre analysis (JAPCC) categorizes the cyber-threats against the drone according to the attacker's intention:

- **Intelligence.** Attackers could intercept and monitor the unencrypted data or information the drone transmits to the ground in order to derive intelligence.
- **Disruption** of the drone. Intentional modification of computer systems by use of malicious code, e.g. viruses, trojans, or worms taking advantage of familiar weaknesses of commercial operating systems.
- **Takeover** of the drone by taking over communication layouts and exploiting the systems bugs, or by way of 'smart entry' into the GCS and its computer systems or drones' avionics.

Harry Wingo (2018) reminds us that events such as the loss of a RQ-170 Sentinel to Iranian military forces on 4th December 2011 or the "keylogging" virus that infected an U.S. UAV fleet at Creech Air Force Base in Nevada in September 2011 show that the efforts of the past to identify risks and harden drones are insufficient. This causing concern over the potential compromise of highly sensitive surveillance capabilities. This incident sparked much research directed towards the hardware and software

security of unmanned vehicle systems. Also, the Predator UAV video stream was hijacked in 2009. Islamic militants used cheap, off-the-shelf equipment to stream video feeds from a UAV.

Next the cyber-attacks against the drone subsystems are described based JAPCC analysis.

1. HUMAN ELEMENT AND SUPPORT ELEMENT

Attacking personnel rather than the drone may be a favorable option for an adversary. Depending on the mission, drone personnel may be working at different locations. So, an adversary may execute the special operations against drone personnel group, which is usually very small in size

2. CONTROL ELEMENT

The Control Element consists of physical infrastructure (external hardware), computer systems (internal hardware) and non-physical software. All may be subject to different types of attack. The physical hardware may be attacked by kinetic weapons while the software may be a target of the non-kinetic attack. The Control Element's computer systems often include Commercial-off-the-Shelf (COTS) components. Identifying the multiple layers of contractors, subcontractors and suppliers contributing to the design or fabrication of a specific chip is difficult; tracing all the contributors for a complete integrated circuit is even more difficult. This widely dispersed supply chain may provide an adversary with opportunities to manipulate or compromised those components or penetrate the distribution chain with counterfeit products. The software components necessary to operate a drone are not limited to the GCS, but also include the drone, satellites and ground stations if applicable, as well as support systems for logistics, maintenance or Processing, Exploitation and Dissemination (PED). This variety provides an adversary with a broad spectrum of possible entry points into the drone system.

Kim Allan et. al states that **hardware attacks** can occur whenever an attacker has direct access to any of the drone autopilot components. An attacker can then corrupt the data stored on-board the autopilot or install extra components that can corrupt the data flow. These types of attacks can be carried out during the maintenance and storage of the drone or during the manufacturing and delivery. An attacker can link directly to the drone autopilot and damage it or reprogram it if he has the means or replace or add components which will give him control over the drone and/or the tactical data collected. Hardware attacks can affect the survivability of the drone, compromise control of the drone, and compromise the tactical data collected by the drone.



In some cases, drones can carry out missions better and cheaper than manned aircraft.



NETWORK ATTACK is most effective if there is regular access to it over time. This can provide the adversary with high quality intelligence that allows the surreptitious installation of malware for future use. Such an electronic backdoor is virtually undetectable by existing defensive technologies. It requires long term maintenance and preservation because of the continuous update process of the defensive systems designed to uncover malicious elements or activity.

SOFTWARE CORRUPTION. Military networks are usually separated from the public internet. This is done to provide the first line of physical or logical defence and protect them from unauthorized remote access. Drone are one of many nodes in the entire network centric environment and countermeasures providing cyber-security are usually applied using a comprehensive approach. Current security software suites offer a variety of methods to counter cyber-attacks. They typically include antivirus, configuration change detection, device control, intrusion detection and prevention, firewall and rogue system detection modules. Many of these modules are COTS applications integrated into the military security system. Simple changes to a malicious program's footprint can reduce its detection even for heuristic search algorithms because they can only defend against threats already known to the software, either by its signature or behavior.

3. DATA LINK

Data links connect drone with the GCS and enable the operators to remotely control the drone and receive transmissions. Possible EW targets for the adversary include the GCS, drone, satellites and satellite ground segments. From the enemy's perspective, the satellite's receiving antenna and the drones GPS antenna appear to be the most promising targets for EW engagements. Regarding the exploitation of transmitted drone signals, multiple discoveries of pirated drone video feeds have proven that

militant groups have adapted their tactics and have regularly intercepted Full-Motion Video (FMV) feeds. Shortly after these security issues were revealed, encryption of FMV streams was designated as a high priority. However, even today, not all currently fielded drone can transmit encrypted video feeds.

Data links connect the drone with the GCS, enabling operators to remotely control the drone and receive transmissions. Data links can be established either by radio for LOS communications or satellites and network nodes for BLOS communications. The radio transmissions may be subject to attack by EW whereas the network nodes may be attacked by means of cyber warfare. Disrupting drone data links by taking out the originators of the transmissions, i.e. the GCS, drone and satellite, or by acquiring access to any of these components by means of cyber-attack is also a viable option for an adversary.

According Kim Allan et. al (2012) **wireless attacks** can occur if an attacker uses the wireless communication channels to alter data on-board the drone autopilot. The worst-case scenario for this attack is if an attacker can break the encryption of the communication channel. Once this occurs, an attacker can gain full control of the drone if the communication protocol is known. Another possibility is an attack such as a buffer overflow that corrupts some data onboard or initiates some event. The most significant danger of wireless attacks is the fact that an attacker can carry out the attacks from afar while the drone is being operated.

Sensor spoofing attacks are directed towards on-board sensors that depend on the outside environment. Examples of such sensors are the GPS receivers, vision, radar, sonar, lidar, and IR sensors. An attacker can send false data through the GPS channels, or blind any of the vision sensors. The drone pilot relies heavily on sensor data for Guidance and Navigation, so corrupted sensor data can be very dangerous, Kim Allan et. al. argues.

5. DRONE CYBER SECURITY

➔ The best way to mitigate a threat is to avoid it; this is also true for the cyber-domain. According to JAPCC analysis suppressing cyber-threats may require pre-emptive infiltration of enemy systems with insertion of malicious code. If necessary, the adversary's cyber-weapon may then be terminated before it can impose a cyber-threat to friendly systems. Hence, pre-emptive cyber-attacks should be considered as an option to suppress enemy cyber-capabilities.

Focus to the human personnel is crucial, JAPCC argues. To prevent corruption, adversary recruitment or blackmail attempts, drone personnel should receive mandatory training to raise the awareness of those issues. Keeping the identities of drone personnel classified could also help to deter those activities. In addition, computer system access policies (both for software and hardware) should be as restrictive as necessary to defend against intrusion attempts or exploitation of human carelessness.

Security software suites and computer system access policies can only provide the foundation for drone computer system protection. JAPCC proposed that personnel with regular access to drone computer systems may be exploited by an adversary to circumvent protective measures, either unwittingly or unwillingly. To minimize the risk of corruption, adversary recruitment or blackmail attempts, regular training that raises the awareness of those issues should be compulsory for drone personnel. Keeping identities of drone personnel classified could also help to avert those types of activities.

Aviation data will be used by drone operations to plan flights. To prevent the possibility of intentional corruption of the data safeguards must be assured. Drone have already inadvertently been infected with malicious software through the careless use of USB memory sticks. According JAPCC in order to minimize the risk of drone computer systems being compromised by viruses, Trojan Horses and other malicious code, security techniques and polices must be improved. Security software suites must use the most current updates to cope with rapidly evolving cyber-threats. Computer system access policies, not only on the software site but also on the hardware site, should be as restrictive as necessary to

defend off intrusion attempts or exploitation of carelessness.

Cyber-security is an extremely fast and adaptive environment. Simple changes to a malicious program's footprint can reduce its detection even for heuristic search algorithms. JAPCC has informed that drone computer systems have already been infected with malicious software. This is most likely due to the prolific use of discs and removable drives. Once discovered, it took several years to disinfect the compromised systems. Eventually, the human factor turned out to be the weakest link for gaining access to even highly secured and physically separated networks.

The supply chain for microelectronics is extremely diffuse, complex and globally dispersed. This makes it difficult to verify the trust and authenticity of the electronic equipment used in the drone. According JAPCC deliberate modification of the product assembly and delivery could provide an adversary with capabilities to completely sidestep any software-based security countermeasures. For example, extraction of encryption keys by carefully modifying the involved integrated circuits has already been demonstrated.

Improvement of drone Command, Control, Communications, and Computer (C4) security must be comprehensive and should encompass the physical components required for drone communication, the computer systems (to include their software packages), the electromagnetic spectrum they operate in, and any personnel with access to the drone. Any of them may be subject to different types of attack and require different efforts to protect them. JAPCC addresses that the financial benefits of incorporating COTS computer hardware should be thoroughly balanced against the inherently superior security of proprietary systems. If COTS systems are preferred, trustworthy supply chains for these hardware components and their sub-components must be ensured. Also, capable, trustworthy and updated security software suites are essential in defending computer networks. Cutting off potential entry points into the drone, e.g. network bridges or removable devices, would further improve cyber security.

Use of the electromagnetic spectrum is required for all drone operations. Ground based links are used for controlling the vehicle, monitoring, and air traffic communications. These links are subject, to varying degrees, vulnerable to jamming, spoofing, and interference. JAPCC suggested that to prevent this from happening, a system of high-integrity, secure data links between the aircraft, the ground control stations, and air traffic facilities will be a fundamental requirement in approving drone operation. Future drone development should focus on reducing radio communications dependency by introducing new means of data transmissions and increasing drone automation.



6. DRONE AS A CYBER-ATTACK PLATFORM

➤ Dan Goodin (2014) described in his article how a drone that can steal the contents of smartphone is developed. Dubbed Snoopy drone can track not only Wi-Fi, but also signals based on radio frequency identification (RFID) and the Bluetooth IEEE 802.15 specifications (Personal Area Network (PAN), Wireless Personal Area Networks (WPAN) communication). Combined with a GPS that correlates signals to the location where they're detected, the capabilities let Snoopy spy not only on phones, tablets, and computers, but also, potentially, on pacemakers, fitness bracelets, smartcards, and other electronics. Plus, the geographically aware Snoopy can also be mounted on a low-cost aerial drone so it can locate and maintain radio contact even when subjects are on a morning run or situated in a high-rise building, a country inn, or some other out-of-the way location.

Dan continued saying that when mobile devices try to connect to the Internet, they look for networks they've accessed in the past. So Snoopy the drone can send back a signal pretending to be networks you've connected to in the past and so the smartphone believes being in trusted Wi-Fi network. When the phones connect to the drone, Snoopy will intercept everything they send and receive. Thus, is possible collect metadata, or the device IDs and network names, intercept usernames, passwords and credit card information. Installing the new cyber intelligence technolo-

gy on drones creates a powerful threat because drones are mobile and often out of sight for pedestrians, enabling them to follow people undetected. When we use different wireless devices and systems, we produce ourselves "digital terrestrial footprint." Based on this footprint, us can be followed, located and attacker has access to our messaging.

In an interview with Pritchard Stephen (2019), Tony Reeves former officer in the UK's Royal Air Force said that "There are plenty of reports to be found of individuals or organizations building or modifying drones to carry RF-based payloads including Wi-Fi tracking, capture and access capabilities – predominantly using Raspberry Pi and Wifi Pineapple devices, but also 2/3/4G network devices. Bluetooth sniffing is also possible. Putting a Wi-Fi access point on top of a building, or inside its perimeter, could allow hackers to listen in to data traffic. Drone operators could also drop a sophisticated microphone into a restricted area for eavesdropping, if technicians can overcome issues of power, weight and range."



Putting a Wi-Fi access point on top of a building, or inside its perimeter, could allow hackers to listen in to data traffic.

CONCLUSION

➤ Security and cyber resilience are a priority area of development to mitigate the risk that drones could be subjected to malicious or accidental takeovers of datalinks leading to accidents, theft or deliberate use of the aircraft to damage infrastructure or hurt civilians. Security requirements of the drone, ground control station, data link infrastructure and even the data must be a fundamental consideration in system design – security by design principle. In addition to being vulnerable to security breaches, drones are also a security threat.

JAPCC argues that the challenge of incorporating security measures into unmanned systems is like that of manned systems, however there are C2 requirements which are unique to unmanned systems and expand their overall requirement for security. The added complexity of these systems and the new technologies they often employ increases the opportunity for adversaries to discover and exploit zero-day vulnerabilities, which may rapidly and severely compromise unmanned systems in new or unexpected ways. This system complexity along with the wide range of capabilities that these systems will be expected to perform will increase the number of attack surfaces for adversaries to exploit. Additionally, it will be challenging to ensure that the underlying architectures of unmanned systems consistently remain in a properly patched and

configured state to eliminate any known cyber vulnerabilities. Cyber is made more challenging by the rapid advancement in the capabilities and design of unmanned systems, which makes fully testing the security of each new iteration extremely difficult. The network needs to be able to handle adding new systems without that affecting the security, availability, throughput, or reliability. Cyber-security teams need to develop new techniques to monitor drones, and to keep confidential information safe.

US DoD (2018) addressed that unmanned systems may be at an even greater risk of cyberattack than traditional systems, due to their autonomy and potential operations in communication and/or GPS-denied environments. This risk is further exacerbated due to the lethal capabilities that some of these systems possess. As a result, cyber expertise and technology must be fully integrated from the onset in the development of unmanned systems architectures. These systems must also be designed with flexibility and the ability to add updates as new cyberattack vectors are identified, and new capabilities are incorporated. For unmanned systems to effectively operate, they must maintain high level cyber security of sensitive information. If adversaries can exploit cyber vulnerabilities in an unmanned system to corrupt any subsystems drones, the result could be a paralysis of the critical infrastructure and vital functions of the society.

Main references

- > DoD (2018). Unmanned Systems Integrated Roadmap 2017-2042, 28 Aug. 2018
- > Goodin D. (2014). Meet Snoopy: The DIY drone that tracks your devices just about anywhere, 26 March 2014
- > Haberl F. & Huemer F. (2019). The Terrorist/Jihadi use of 3D-Printing Technologies: Operational Realities, Technical Capabilities, Intentions and the Risk of Psychological Operations, in proceedings of the ICCWS 2019, 28 February - 1 March 2019, Stellenbosch, South-Africa
- > Hartmann K. and Steup C. (2013). The vulnerability of UAVs to cyber-attacks – an approach to the risk assessment, in proceedings of the 5th International Conference on Cyber Conflict.
- > JAPCC. (2014). Remotely Piloted Aircraft Systems in Contested Environments A Vulnerability Analysis, September 2014
- > Kallenborn Z. (2018). The era of the drone swarm is coming, and we need to be ready for it, Modern War Institute at West Point, October 25, 2018
- > Kim A., Wampler B., Goppert J., Hwang I., Aldridge H. (2012). Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles, Infotech@ Aerospace
- > McMullan T. (2019). How swarming drones will change warfare, BBC News, March 16, 2019
- > MoD. (2015). Preliminary Assessment for Replacing the Capabilities of the Hornet Fleet Final Report, 8.6.2015
- > Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (2016). Report of the Defense Science Board Summer Study on Autonomy, Washington, D.C., June 2016
- > Papireddy T. (2015). Tracking and Monitoring Unmanned Aircraft Systems Activities with Crowd-Based Mobile Apps, University of Nevada, USA, 1 May 2015
- > Payne T. (2017). Lethal Autonomy What It Tells Us About Modern Warfare, Air & Space Power Journal, Winter 2017
- > Pritchard S. (2019). Drones are Quickly Becoming a Cybersecurity Nightmare, Threatpost, 22 March 2019
- > SESAR. (2016). European Drones – Outlook Study –Unlocking the value for Europe, November 2016
- > Wingo H. (2018). Beyond the Loop: Can Cyber-Secure, Autonomous Micro-UAVs Stop Active Shooters? in proceedings of the 13th International Conference on Cyber Warfare and Security ICCWS 2018, 8 - 9 March 2018

WELCOME TO THE 1ST DRONE CONGRESS IN HELSINKI

1-3 OCTOBER 2019, EXHIBITION CENTER

The Helsinki Drone Congress brings together internationally recognized executives, leading experts, drone professionals, and manufacturers from all around the world to exchange and share their experiences. Furthermore, the Congress will serve as a platform to conduct extensive discussions relevant to the UAV Industry, cooperation enhancement, and partnerships building.

In collaboration with



Cyberwatch
Finland

Aeronautics Group

DRONE CONGRESS CONNECTS

➤ Drone Congress connects drone experts, cyber security experts, drone Olympics teams, buyers, sellers, researchers, universities, companies, decision makers, entrepreneurs, investors, top speakers in three day conference

We are the Gateway to the EU Drone market, connecting the whole world in a safe, reliable and stable way

Finland - Security by design - Drone and Cyber Security - Products and Solutions should be Developed with safety in Mind

Finland's unique know-how in cyber security is a clear competitive advantage for drone industry

MEET – CONNECT – SHARE – LEARN BUILD TRUST

FINLAND'S STRENGTHS
Technological expertise, innovation and research combined with liberal regulations for testing UAV's and stable way

NETWORK
Meet WUAVF European Chapters and Asian delegates

BENCHMARK
Share experiences – create business opportunities – enhance cooperation



WHY TO PARTICIPATE?

✓
To meet potential customers who are looking for your services

✓
To explore the possibilities to expand your business to EU market

✓
To buy Finnish solutions

✓
To sell to Finnish companies and organizations

✓
To develop together

✓
To participate in research

✓
To create own testbed in Finland

✓
To share thoughts about innovations

✓
To hear in which areas we already are testing drones

READ MORE:



DRONES WILL BE HAVING A CRUCIAL ROLE IN DEVELOPING SERVICES AND INFRASTRUCTURES IN THE NEAR FUTURE

by **Aapo Cederberg**, CEO, Cyberwatch Finland, Chairman of the Cyber Security Committee of World UAV Federation (WUAVF)

➤ Drones will be playing a growing role in the critical infrastructure environment. They have numerous tasks in critical infrastructure maintenance and protection. At the same time CI must be able to deal with the new and emerging threat of drones. The most significant risks tend to be physical and electronic attacks. Security and cyber resilience must be a priority area of developing and mitigating the risk of drones.

We must be able to avoid malicious or accidental takeovers of data links leading to accidents or deliberate use of the aircraft to damage civilian infrastructures. Security requirements of UAVs ground control station, data link infrastructure and data must be fundamental in designing the whole ecosystem. The 'security by design' principle should be a must for the new solutions. The international community should be able to provide recommendations and basis requirements for cyber security of the whole drone ecosystem. Cyber security should be a priority area of the security arrangements of the UAVs.

CONFERENCE ROOM 201

1. DRONE DAY 1st oct

- 9:10 Opening speech** by Mr. **AAPO CEDERBERG**, CEO, Cyberwatch Finland, Chairman of the Cyber Security Committee of World UAV Federation (WUAVF)
- 9:25 Keynote: Current Development Status and Prospects of China's UAV Industry**, Mr. **JINCAI YANG**, Chairman of the WUAVF
- 10:05 Keynote: Drones in cyber security environment**, Dr. **MARTTI LEHTO**, Professor, Cyber Security, Col G.S (ret.) Faculty of Information Technology, University of Jyväskylä, Adjunct professor in National Defence University, Air and Cyber warfare
- 10:35 Keynote: Drones – A rising threat or an opportunity**, Mr. **NIR WEISSER**, Aeronautics Ltd.
- 10:55 Cyber security risk management in aviation and drones**, Mr. **TOMI SALMENPÄÄ**, Chief Adviser, Aviation Cybersecurity, Finnish Transport and Communications Agency Traficom Aviation (CAA Finland)
- 11:15 The Opening Ceremony** of the UAV Finland Chapter, Mr. **PERTTI JALASVIRTA**, Cyberwatch Finland partner, President of Finland Chapter of World UAV Federation (WUAVF)
- 11:45** Mr. **ANTE GLIBOTA**, Vice President of European Academy of Sciences, Arts & Humanities (EASAL), International Consultant for World UAV Federation
- 12:15 - 13:15 LUNCH BREAK**
- 13:15 The impact of EU legislation and national leeway**
Ms. **ELINA IMMONEN**, Director of Safety and Security Unit at the Finnish Ministry of Transport and Communications
- 13:35 Drone Tournament 2019**, Mr. **MIKKO JÄRVILEHTO**, CEO, Ultrahack
- 13:55 Collaborative drone research and development to boost your business** Mr. **HANNU KARVONEN**, Senior Scientist, Ecosystem Lead for Autonomous Systems, VTT Technical Research Centre of Finland
- 14:15 Michigan project**, Mr. **KWON HEE-CHOON**, Vice Chairman of Korea Digital convergence agency, Visiting Professor of Hanyang Cyber University, Secretary General of National Agency of Cognitive Science
- 14:35 GOF U-space and the integration of drone and aircraft in the same airspace**, Mr. **JONAS STJERNBERG**, SVP Robots. Expert, CEO BVdrone Oy, Chairman of RPAS Finland ry
- 14:55 – 15:25 BREAK**
- 15:25 Data Rain drone swarming and secure connectivity platform** Mr. **ARIMO KOIVISTO**, Chief Commercial Officer and partner, XXLSEC Oy
- 15:45** Mr. **JAN LINDBERG**, CEO, Skydata Ltd.

CONFERENCE ROOM 207

2. DRONE DAY 2nd oct

- 13:30- 14:00 Networking coffee**
- 14:00 Drones in Smart City - Case Tampere** **Hiedanranta**, Mr. **ANTTI PERTTULA**, PhD, Principal Lecturer, Systems Engineering, Head of Aircraft Engineering Studies Tampere University of Applied Sciences
- 14:20 Keynote:** Mr. **NIR WEISSER**, Aeronautics Ltd.
- 14:30** Mr. **JUKKA HANNOLA**, Chief Adviser to DGCA Chairman – Joint Authorities for Rulemaking on Unmanned Systems (JARUS), The Transport and Communications Agency Traficom
- 14:50 Smart City - Carbon Neutral Drone Solutions in Southern Finland**, Ms. **HEIDI HEINONEN**, Project Manager, Forum Virium Helsinki
- 15:10** Mr. **STEPHEN SUTTON**, CEO, The Fly-by Guys, Operations Manager at Fleetonomy.ai
- 15:30 Staying aware and mobile in digital world!**, Mr. **MARKUS RANNE**, Program Manager, Business Finland
- 15:50- 16:50 Helsinki Drone Tournament**
Teams x 3 pitching & Company showcases

CONFERENCE ROOM 207

3. DRONE DAY 3rd oct

- 8:30- 9:00 Networking breakfast**
- 9:00 Drone based remote sensing in forestry – State-of-the-art and future prospects**
Ms. **EIJA HONKAVAARA**, D.Sc. (Tech.), Research Manager, NLS National Land Survey of Finland
- 9:20 Keynote:** Mr. **NIR WEISSER**, Aeronautics Ltd.
- 9:40 Use of drones in forest legislation enforcement - benefits and challenges**, Mr. **LAURI HAATAJA**, Project Manager, Metsäkeskus
- 10:00 Far and back – drones to monitor atmosphere and environment**, Ms. **ANNE HIRSIKKO**, Drone-borne atmospheric observations, Climate Change Research, Finnish Meteorological Institute
- 10:20 How can research help with your drone-related cybersecurity challenges**, Mr. **JARNO SALONEN**
Senior Scientist, VTT Technical Research Centre of Finland
- 10:40 Wuudis Service - Digitalizing Forestry by harnessing the power of Big-Data**, Mr. **SEPPO HUURINAINEN**, CEO, Wuudis Solutions Ltd
- 11:00 Drones in CIP**, Mr. **MATS FAGERSTRÖM**, Business Security Manager, Helen Oy, HSV Oy, HET Oy
- 11:20- 12:40 Helsinki Drone Tournament 2019**
Teams x 5 pitching & Company showcases
- 12:40 The story continues**, Mr. **PERTTI JALASVIRTA**, President of Finland Chapter of World UAV Federation (WUAVF)



AAPO CEDERBERG

CEO, Cyberwatch Finland, Chairman of the Cyber Security Committee of World UAV Federation (WUAVF)

Opening speech



ARIMO KOIVISTO

An experienced cyber security and secure connectivity professional with military background. Arimo is working in several drone and autonomous robotic connectivity projects globally. Future swarming in robotics requires new technologies to enable real autonomy and shared computing technologies. Data Rain is a solid technology for real time shared knowledge requirement in swarming robotics and artificial intelligence solutions.



MARTTI LEHTO

Dr. Martti Lehto, (Military Sciences), Col (GS) (ret.) works as a Cyber security professor in the University of Jyväskylä in the Faculty of Information Technology. Martti has over 40 years' experience as developer and leader of C4ISR Systems in Finnish Defence Forces. Now he is a Cyber security and Cyber defence researcher and teacher and the pedagogical director of the Cyber Security MSc. program. He is also Adjunct professor in National Defence University in Air and Cyber Warfare. He is leader of the CyberSecFIN cybersecurity ecosystem of the Allied ICT Finland (AIF). He has over 130 publications, research reports and articles on the areas of C4ISR systems, cyber security and defence, information warfare, air power and defence policy. Since 2001 he has been the Editor-in-Chief of the Military Magazine.



NIR WEISSER

Mr. Nir Weisser is Aeronautics BD and marketing director for Finland. Holds a BSc of engineering and MBA. Mr. Weisser has a vast experience, more than 20 years in both manned and unman platforms as internal pilot, system engineering and BD/sales director. Aeronautics is a leading world comply to develop and produces (one stop shop) variety of drones VTOL solutions (multi rotor – VTOL capabilities) as well as fix wings starting from tactical applications (10KG) up to MALE (2000 kg) for all markets: Civil, HLS and Defense.



STEPHEN SUTTON

Stephen has been an active participant in the Finnish UAV community for over 2 years. A popular drone photographer, one of the founders of The Fly-By Guys, and now Operations Manager at Fleetonomy.ai, Stephen is helping the industry find its voice for good and safety in Finland, and beyond.



ELINA IMMONEN

Ms. Elina Immonen works as Director of Safety and Security Unit of the Finnish Ministry of Transport and Communications. The Safety and Security Unit is entrusted with matters relating to privacy protection and the security and confidentiality of transport and communications services.

Ms. Immonen holds a Master's Degree in Social Sciences as well as a Master's Degree in Laws. Since 2006, she has held various specialist and executive positions in several Finnish ministries. During her career as a public servant, she has led and taken part in many legislative and other reformative projects.



TOMI SALMENPÄÄ

Tomi Salmenpää is a Chief Adviser in Aviation Cybersecurity to Traficom, Civil Aviation Authority (CAA) Finland. During his 7-year tenure, Tomi has been working with approval, certification and oversight of airlines continuing airworthiness. In his current role, he focuses on the implementation of cybersecurity to the civil aviation system, internationally and nationally. Tomi contributes actively to the international cooperation e.g. in ICAO, EASA, ECAC and ENISA cybersecurity activities, developing future regulation, - best practices and holistic risk management methods to aviation. At national level, a close cooperation with stakeholders provide support to manage cybersecurity appropriately in the continuously evolving cyberspace. He also works on a doctoral thesis, which researches methods for holistic cybersecurity risk management in aviation. Before Trafi, Tomi worked several years in different airworthiness positions in airlines.



EIJA HONKAVAARA

Dr. Eija Honkavaara works as a Research manager at the Finnish Geospatial Research Institute in the National Land Survey (FGI). She has over 10 years experience in drone based remote sensing. She leads the FGI's DroneFinland research team that has developed several pioneering drone-based remote sensing solutions. In forestry applications her research focuses the forest inventory and forest health analysis using photogrammetric and spectrometric technologies.



LAURI HAATAJA

Project manager at Finnish Forest Centre in project Digitization of forest legislation enforcement. Master's Degree in Forestry and almost 10 years working experience with quality control methods of silviculture first in Natural Resources Institute Finland and later in Finnish Forest Centre. Wide aim of ongoing project is to develop and pilot new solutions for collecting, producing and sharing forest data in support of Finnish forest legislation enforcement. Main current task and interest is to find out what forest parameters can be measured by agile drone-based methods.



MIKKO JÄRVILEHTO

Mikko Järvillehto, Founder and Director of the Ultrahack (Futuretournaments Oy). He is a specialist in challenge contests and hackathons, innovation management and commercialization. Järvillehto has organized close to 100 innovation challenges with various industries to drive both digitalization and exchange of talent in global scale. He is the inventor of the Drone Tournament, which is an drone innovation challenge competition that introduces new services & ways to use various technologies for e.g. in farming, forestry, rescue services, logistics, traffic and maintenance. Järvillehto is also an author for over 40 scientific publications and co-founder of three startups.



HANNU KARVONEN

"Hannu Karvonen works as a Senior Scientist and Ecosystem Lead for Autonomous Systems at VTT Technical Research Centre of Finland Ltd. He is currently the Coordinator of an innovation ecosystem called Research Alliance for Autonomous Systems (RAAS, www.autonomous.fi). RAAS includes 200 researchers from 27 research organizations and one of RAAS' key application domains is drones. Hannu has a Master's Degree in Economics and he is currently finishing his PhD in Cognitive Science. He has 16 years of work background in usability research and user interface design both from the academia and industry. His previous research work has focused on human factors in complex systems, user experience design in safety-critical environments and the development of autonomous systems."



ANTTI PERTTULA

Dr. Perttula has over 10 years' experience in aeronautical engineering in the Finnish Air Force, ICAO and academia. His main research areas include quality management, testing, fast product development, Systems Engineering, flight mechanics, measuring technology and avionics. He has started and participated in many drone related projects like City Logistics, Drone Specialist and designing & prototyping VTOL drones. He is also giving lectures in Aeronautical subjects including drones. In addition, Perttula has headed NASA's Epic Challenge Mars project where students are solving very difficult problems related with setting up permanent habitat on Mars. He has also gained long international experience while living and working in Asia, Africa and Europe.



JONAS STEJRNBORG

"Jonas Stjernberg is Senior Vice President at Robots Expert Finland Oy (REX). REX is a European consultancy focused on drones, on Urban Air Mobility and on digitalizing aviation. Jonas has a long background as a senior change management and strategy professional bridging the gap between people and technology. Jonas is the Chairman of RPAS Finland ry, the industry association for professional UAV stakeholders in Finland as well as the CEO of BVdrone Oy, a drone operator focused on demanding remote sensing and environmental monitoring drone operations. Jonas is one of the core drivers behind GOF U-space, an EU-supported Estonian-Finnish Very Large drone Demonstration project on the next step in integrated aviation. Jonas is also involved in 5G!Drones a H2020 project focused on developing metrics and guidelines for the use of 5G networks in drone use cases. Robots Expert is the EIP-SCC Urban Air Mobility ambassador in Finland, and the company has authored a comprehensive Droneguide for Cities (in Finnish)."



HUURINAINEN SEPPO

Mr Seppo Huurinainen is the establisher and CEO of Wuudis Solutions Oy, a forerunning company in forest digitalisation. Wuudis Solutions harnesses the power of big data through integrating Wuudis with multiple forest big data sources in standardized way and implements intelligent algorithms to make forest management and monitoring simple, systematic, autonomous and cost-effective. Mr. Huurinainen holds a Licentiate Degree in Forestry as well as a Licentiate Degree in Ecological Botany. His international career has included long-term project tasks in Indonesia and Mozambique.



PERTTI JALASVIRTA

The Opening Ceremony of the UAV Finland Chapter

Pertti's + 30 years of work history is proof of his solid background of professional expertise in government affairs, resource management, administrative management, planning of organizational development in military medicine, education and hospital relations, as well as CBRN protection and training of security, cyber skills within education industry, the healthcare and medical industry.

Pertti has extensive experience at the executive group level and board level in multiple companies both in Finland and transnationally.

Pertti is also a decorated Medical Service Corps Reserve Warrant Officer, and have been responsible for the development, training and testing of new medical equipment and emerging technologies for the Finnish Defense Forces during 1983 to 2010. Additionally, he has played a major role in the development of techniques, procedures and logistical integration of procured medical equipment for the Finnish Defense Forces.

Pertti is also Associate Fellow at Geneva Center for Security Policy, GCSP and owner and CEO of Jalasvirta Group, founding partner of Cyberwatch Finland Oy

Today, Pertti focus primarily on using his wide professional experience to provide consulting services for the Military, Cyber Security Strategy, Cyber Education, Cyber in Healthcare and Government business segments.



MR. JARNO SALONEN

Mr. Jarno Salonen is working as a Senior Scientist in the Cybersecurity team at VTT Technical Research Centre of Finland Ltd - the largest multi-technological research organisation in Northern-Europe. He has a professional background of over 17 years in making the digital world a better place for ordinary users especially in the areas of cybersecurity, privacy and development of electronic services. His recent activities include among others the definition of cybersecurity competences for the Finnish Government; "Cyber security competencies in Finland - Current state and roadmap for the future" (2015-2016). In 2017 he coordinated two projects for the Prime Minister's Office in Finland; "Opportunities and benefits of blockchain technology in social and health care" and "Competence-based security of supply to guarantee the technological and industrial basis of Finland's defence". Currently he is the Finnish country coordinator for ITEA3 project "17032 CyberFactory#1" lead by Airbus CyberSecurity and addressing opportunities and threats for the Factory of the Future (FoF). He is the representative of VTT in one of the working groups in ECSO - European Cyber Security Organisation, a member of the Finnish Information Security Cluster (FISC) management team and his work has been published in several scientific journals and conferences.



KWON HEE CHOON

10 year experience as Associate Professor at Suwon Women's College
 Korean App award Judge
 Director of Korea Electronic publishing agency(present)
 Vice Chairman of Korea Digital convergence agency(present)
 Visiting Professor of Hanyang Cyber University(present)
 Secretary General of National Agency of Cognitive Science (present)

Dr. Hee-choon Kwon is a professor of Digital Media Department at the Suwon Woman's College, Suwon. He received his Ph.D. from SKKU and eventually earned his Professor job. After his fifteen-year career as a teaching there, Dr. Kwon decided it was time for a change of a Job for Digital Convergence Agency, where he was offered as Vice President. In addition to teaching and Research, Dr. Kwon is a regular contributor to National Police University and Book Writing of Police Drone. He recently collaborated on making manuscript and publishing with friends and colleagues,



HEIDI HEINONEN

Heidi works as project manager at Forum Virium Helsinki co-creating urban futures with the city, the science community, residents and companies.

She holds a M.Sc. degree in Economics for University of Sorbonne, Paris.

Sustainability is her passion; she lives as she talks and is a driven promoter of carbon neutrality and circular economy, at home, in her neighbourhood and professional life.

She is a change maker and organisation developer with experience in leadership from the creative industry focusing on sustainable & lean development.



ANNE HIRSIKKO

Dr. Anne Hirsikko is a head of group for Weather radars and atmospheric profile measurements in Finnish Meteorological Institute (FMI). Her ambition is to utilize new innovative measurement techniques to fulfil gaps in atmospheric profiling both in operational observation service and research. She leads UAV team in FMI. The team includes climate and air quality scientists making drone-borne atmospheric observations and meteorologists developing tailored weather services for UAV.



MARKUS RANNE

Markus Ranne is the Program Manager of the New Space Economy program at Business Finland. Previously he has worked in various project functions at Business Finland, Finpro, European Space Agency and IVO Power Engineering. He has a Master's degree in electrical engineering from Helsinki University of Technology and a MBA from Aalto University.

The New Space Economy program aims to benefit from the growth potential of international space business. The program offers funding, networks and internationalization services for developing global space business, and funds industry disrupting startups, growth-seeking manufacturing companies and businesses focused on data utilization. Drones are relevant to the New Space Economy program especially in the situational awareness domain.

Business Finland is the Finnish innovation funding, trade, investment, and travel promotion organization, headquartered in Helsinki.

New Space Economy program:
www.businessfinland.fi/en/space
 Business Finland: www.businessfinland.fi/en

Space Finland - latest on the Finnish space know-how:
www.spacefinland.fi



JUKKA HANNOLA

Mr. Hannola is the Chairman of Joint Authorities for Rulemaking on Unmanned Systems (JARUS). He joined CAA Finland in 2011. In his role Mr. Hannola is in charge of the drone sector. He is a member of ICAO RPAS panel and EASA drone rule making task 230. He also contributes to several other EU-level working groups including UTM/U-Space regulation development. Prior to his current position he served as a development manager in CAA and at the same time he was the manager of the Airspace 2014 - project, which included major restructuring of Finnish airspace paving the way for the free route airspace -concept. He was also in charge of ATC and Airspace related performance development plan.

Formerly, before joining the Finnish Transport Safety Agency Mr. Hannola served as a deputy manager of Flight Ops/Dispatch office in a business jet company. Prior to this assignment he served as an air traffic controller in a Finnish state owned air navigation service provider Finavia Oyj. Mr. Hannola is a graduate from the Avia College, a state owned aviation institute. He is an air traffic controller and holder of glider and private pilot licenses. He also holds a Master's degree in Administrative Sciences from the University of Tampere. He has been also a model aircraft and drone enthusiast for the past 25 years.

CYBER SECURITY NORDIC

2-3 October 2019
Messukeskus Helsinki

THE MOST SIGNIFICANT EVENT OF
CYBER SECURITY IN NORTHERN EUROPE

➤ Cyber Security Nordic in Helsinki is a conference introducing keynotes and panels focusing on the problem solving strategies and solutions for cyber security professionals.

Cyber Security Nordic is divided into exhibition, conference and meeting area.

If you are in IT or cyber security this is the key meeting place for you. And CEO! If you go to ONE event this year, make it this one!

EDITORIAL
FAVORITES AT
THE CYBER
SECURITY
NORDIC EVENT

Wednesday Oct 2

9:00-9:10 **Welcome! To do list - TOP 5 lessons to learn, Kimmo Rousku,**
General Secretary, Population Registration Centre, Stage 2

Politics of Cyber

9:15-9:45 **Who is responsible for your cybersecurity? Aaron Boyd,**
Managing Partner of Welchman Keen

9.45 - 10.30 **Stuxnet and Beyond: Digital Weapons and the Future of Our
Cities, Kim Zetter**

OR

9.10 - 9.50 **It's GDPR-time - 495 days behind, Anu Talus**

11.15 - 11.45 **The Impact of Russian Politics on the Cyber World?**
Mark Galeotti

Senior Associate Fellow at the Royal United Services Institute

Economy of Cyber

13.45 - 14.15 **The Business Impact of Cyber Attacks from the Hackers
Point of View, Itay Savion, Director of Sales**

Thursday Oct 3

13.30 - 14.15 **Keynote: Future of Cyber and Predictions for 2020,**
Rik Ferguson

14.15 - 15.00 **Keynote: Building the security operations center of
tomorrow - better insights with compound detection,**
Diana Kelley,
Cybersecurity Field CTO

15.30 - 16.15 **Keynote: Security and Privacy in a Hyperconnected World,**
Bruce Schneier

CYBER
SECURITY
NORDIC



Wednesday Oct 2

9.00 – 9.15 Opening
STAGE 1

Politics of Cyber

- 9.15 – 9.45 Who is responsible for your cybersecurity?**
Aaron Boyd, Managing Partner of Welchman Keen
- 9.45 – 10.30 Stuxnet and Beyond: Digital Weapons and the Future of Our Cities**
Kim Zetter

BREAK

- 11.15 – 11.45 The Impact of Russian Politics to the Cyber World?**
Mark Galeotti, Senior Associate Fellow at the Royal United Services Institute
- 11.45 – 12.15 Cyber Awards**

LUNCH BREAK

Thursday Oct 3

9.00 – 9.05 Opening
STAGE 1

Reality of Cyber

- 9.05 – 9.35 CISO's cheat sheet to OT security**
Robert Valkama, Senior Information Security Consultant, industrial information security, Nixu Oyj
- 9.35 – 10.20 Keynote: Cyber Reality meets Future – examples and war stories**
Roe Schreiber, Security Principal Director, Accenture Security (Maglan) and Elad Segev, Security Principal Director, Accenture Security (Maglan)

BREAK

- 11.00 – 11.45 Leadership challenges in modern multicultural societies: The human role in cyber security**
His Holiness A.V. Bhakti Vidya Purna Swami, D.Theol.h.c., Prof.Div. (alias Alan Ross Wexler)
- 11.45 – 12.30 Keynote: Life after the breach you didn't detect**
Tom Van de Wiele, Principal Cyber Security Consultant, F-Secure

LUNCH

Wednesday Oct 2

Economy of Cyber

STAGE 1

- 13.45 – 14.15 The Business Impact of Cyber Attacks from the Hackers Point of View**
Itay Savion, Director of Sales & Business Development at XM Cyber
- 14.15 – 15.00 Keynote: Are you ready for growth? Security & Privacy in M&A**
Kauko Storbacka, Advisory and Deals Leader, PwC Finland

BREAK

- 15.45 – 16.15 Disruption – the limits of your imagination are not the limits of the world**
Perttu Pölönen – inventor, entrepreneur and composer

16.15 – 17.00 Boards view on cyber security
How important topic Cyber Security is at Boards' agenda? What is boards responsibility? What kind of information board is expecting from cyber security? Is there a wider need for Cyber Security knowledge in Boards generally? Are we seeing that Cyber Security expertise is a selection criteria in the future when nominating board members? Panel is taking a deep dive into board members daily live and the challenges they are facing when executing their duties in major companies.

Panelists and board:

- Anu Nissinen**, DNA Oyj, Siili Solutions Oyj, Viestilehdet Oy, Finnish Fair Corporation, Rantalainen Group Oy, Finnish Film Foundation.
- Esa Rautalinko**, Patria Oyj, Millog Oy, Nammo AS, Nest Capital GP
- Arto Rätty**, Senior Vice President, Fortum Corporation, Lieutenant General (Ret.), Aalto University Executive Education Oy, Suomi Gas Distribution Holding Oy, AC Cleantech Management Oy, TT Foundation, Fortum Art Foundation, Urlus Foundation, Fennovoima Oy, Savonlinna Opera Festival, Destia Oy, Harri Koponen, Chief Commercial Officer Nortol AS & CEO of Nortol Oy

17.00 – 18.00 Cyber Wine
Partners' Area

Thursday Oct 3

Future of Cyber

STAGE 1

- 13.30 – 14.15 Keynote: Future of Cyber and Predictions for the next decade**
Rik Ferguson
- 14.15 – 15.00 Keynote: Building the security operations center of tomorrow – better insights with compound detection**
Diana Kelley, Cybersecurity Field CTO

BREAK

- 15.30 – 16.15 Keynote: Security and Privacy in a Hyperconnected World**
Bruce Schneier

Wednesday Oct 2

STAGE 2

- 9.00 – 9.10 Welcome! To do list – TOP 5 lessons to learn**
Kimmo Rousku, General Secretary, Population Registration Centre
Tietosuoja uuden teknologian hyödyntämisen ja palveluiden mahdollistajana
- 9.10 – 9.50 It's GDPR-time – 495 days behind**
Anu Talus, apulaistietosuojavaltuutettu, tietosuojavaltuutetun toimisto
- 9.50 – 10.30 Onko tietosuoja meno vai investointi?**
Reijo Aarnio, tietosuojavaltuutettu, tietosuojavaltuutetun toimisto

COFFEE BREAK

- 11.15 – 12.15 How to build digital trust in the society?**
Digital identity as fundamental building block
Joonatan Henriksson, Nixu Cybersecurity / SisulD
Real-time economy needs data connected to identities
Pirkka Frosti, Digital Living International
MyData based digital services ensure privacy
Mika Huhtamäki, Suomen Tilajavastuu & MyData

LUNCH

Thursday Oct 3

STAGE 2

- 9.00 – 9.05 Opening**
Suomen Kyberturvallisuus tänään
- 9.05 – 9.30 How to strengthen co-operation in cyber domain – a case for Comprehensive Security Approach**
Jukka Juusti, Permanent Secretary, Chairman of the Security Committee
- 9.30 – 9.55 The Just Published Finnish Cyber Security Strategy 2019 – highlights**
Vesa Valtonen, General Secretary of Security Committee
- 9.55 – 10.20 Protection of Finnish 2019 Elections – Information and Cyber Environment**
Antti Sillanpää, Senior Researcher, Secretariat of Security Committee

COFFEE BREAK

- 11.15 – 11.45 How to measure Cyber / Digital security? How we are doing in Finland – from global to local organisational level?**
Kimmo Rousku, General Secretary, Population Registration Centre
- 11.45 – 12.30 Kybersää ja pitkän ajan ennuste 2020-luvulle**
Jarna Hartikainen, päällikkö, Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus

LUNCH

Wednesday Oct 2

2020-luvun digitaalinen toimintaympäristö – valtavat mahdollisuudet, entä uhat?

STAGE 2

- 13.45 – 15.00 Case Kokemäki – yhden kyberhyökkäyksen anatomia –paneeli**
Moderatoori: Kimmo Rousku, VAHTI-pääsihteeri, Väestörekisterikeskus.
Panelistit: Mikko Löfbacka, hallintojohtaja, Kokemäen kaupunki | **Mikko Rauhamaa**, Kyberrikostorjuntakeskuksen päällikkö, Keskusrikospoliisi | **Reijo Aarnio**, tietosuojavaltuutettu

COFFEE BREAK

- 15.45 – 16.15 Tiedonhallintalaki astuu voimaan 1.1.2020 – miten tämä vaikuttaa koko julkisen hallinnon ja elinkeinoelämän toimintaan – tietoturvaluottelu?**
Sami Kivivasara, lainsäädäntöneuvos, yksikön päällikkö valtiovainministeriö

- 16.15 – 17.00 Menneisyyden opit – entä mitkä uutiset järkyttävät meidän turvallisuutta 2020-luvulla ja kuinka varaudut niihin?**
Panelists: Catharina Candolin, TKT, kyberpuolustuksen erityisasiantuntija, Puolustusvoimat | **Erka Koivunen**, tietoturvaohjaaja, F-Secure | **Martti J. Kari**, yliopistonopettaja, eversti (evp)

17.00 – 18.00 Cyber Wine
Partners' Area

Thursday Oct 3

Miten organisaatiosi pystyy kehittämään turvallisuuttaan?

STAGE 2

- 13.30 – 14.15 Tuoteturvallisuuden trendit ja viranomaisnäkökulma**
Saana Seppänen, erityisasiantuntija, Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus
- 14.15 – 15.00 Miten Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelman JUDO-hanke edistää koko yhteiskunnan turvallisuutta? Mitä hyötyjä hanke tarjoaa yrityksille, entä kansalaisille?**
Kimmo Rousku, Erja Kinnunen, Juha Kirves and Hanna Heikkinen, Väestörekisterikeskus

COFFEE BREAK

- 15.30 – 16.15 Keynote: Security and Privacy in a Hyperconnected World**
Bruce Schneier

A HEAD OF ITS TIME

Aeronautics Group variety of drones provides a wide range of solutions for defense, HLS and border protection missions.

text: Aeronautics Group



AERONAUTICS GROUP LTD. was established in the end of in 1997. Since then Aeronautics acquired over 3 decades of experience in providing integrated turnkey solutions based on unmanned systems platforms, variety of payloads and communications for defense and civil applications.

Until today Aeronautics is serving over 75 clients in more than 55 countries around the globe.

Designed as leading-edge UAS-based solutions, Aeronautics Group systems offer operationally proven solutions for Intelligence, Surveillance and Reconnaissance (ISR) systems requirements as well as civil applications such as logistics, smart cities, emergency, engineering and architecture.

As a pioneer in the field of unmanned aerial systems, Aeronautics broad product portfolio has demonstrated excellent performance and operability. Backed by continuous research and development, these systems are built on three decades of technological and operational experience.

Through our in-house capability (one stop shop) as an UAS/Drone integrator with specialist subsidiaries and technology partners, we offer a complete range of sub-systems that support all the mentioned missions above. Aeronautics Group systems are based on building blocks of platforms, flight computers, communication, sensors and navigation thus enable us to modify and tailored our systems to meet our clients need and requirements. The product portfolio is combine from four main solutions:

- 1. ORBITER FAMILY** is Aeronautics tactical fix wing platforms starting from 10 up to 50 Kg all no need of a runway. Gained over 300,000 operational flight hours in verity of environments including challenging weather conditions (including Finland).
 - a. Orbiter 2B (10Kg Max takeoff weight) – super tactic solution, operated by only 2 team members. Flight endurance is up to 4 hours and capable to carry 1.5kg of payloads.
 - b. Orbiter 3B (30Kg Max takeoff weight) –tactical solution, operated by only 3 team members. Flight endurance is up to 7 hours and capable to carry 5.5kg of payloads.

Both orbiter 2B and 3B are electric engine driven, thus the acoustic signature is very low and can been flown in low altitude without being discovered.

- c. Orbiter 4 (50Kg Max takeoff weight) – tactical solution, operated by only 3 team members. Flight endurance is up to **24 hours** and capable to carry multiple payloads simultaneously up to 12kg.

The Orbiter 4 has a silent combustion engine that provides capabilities that usually can be seen at much bigger and more expensive platforms.

All the orbiter family has a very small logistic footprint, easy to maintain and to operate.

- 2. UAVS** – from 230 kg up to 2000kg for long endurance with high capabilities of payload caring.
 - a. Aerostar (230Kg Max takeoff weight) – Flight endurance is up to 12 hours and capable to carry multiple payloads simultaneously up to 50kg with over 300,000 of operational flight hours.
 - b. Dominator (1910Kg Max takeoff weight) – Aeronautics converted the Diamond DA 42 into a drone thus it is fully redundant platform including tween engines and all weather operation. Flight endurance is up to **20 hours** and capable to carry multiple payloads simultaneously up to 373kg.
- 3. MULTI-ROTOR / VTOL PLATFORM**
 - a. Pegasus 120 (120Kg Max takeoff weight) – operated by only 2 team members. Flight endurance is up to 1 hours and capable to carry 45kg of payloads.
 - b. Pegasus 15 (15Kg Max takeoff weight) – operated by only 2 team members. Flight endurance is up to 1 hours and capable to carry 8kg of payloads.
 - c. Pegasus 5 / Drone Box (5Kg Max takeoff weight) – operated by only 1 team members. Flight endurance is up to 1 hours and capable to carry 2.5kg of payload. Remote monitoring which enables command and control the drone from a farther site.

” Aeronautics Group puts a lot of effort into the unmanned interface so it is as intuitive as possible to provide communality between the systems.



Orbiter 4

Dominator

Pegasus 120

Additional advantages that are important to be aware of is that all of our systems are "Cyber to Design" with immune communication to prevent taking over the control by unauthorized entities.

Aeronautics Group puts a lot of effort into the unmanned interface so it is as intuitive as possible to provide communality between the systems. In addition, other components such as the communication and control station are also hold communality capabilities between the systems in order to simplify maintenance and logistics aspects.

- 4. **COMPREHENSIVE AND TAILORED** made solutions for different kinds of assets and facilities such as airports, oilrigs, power plants/lines etc. including:
 - a. Mission and Communication Control
 - b. Auto Detection of any kind of threats including **anti-drones**
 - c. Early Warning
 - d. Situation Awareness
 - e. Situation Analysis

It is known that the future belongs to the unmanned platforms and Aeronautics Group is already taking into considerations many aspects that will affect the usage of drones, one of them is the regulation aspect led by FAA that will take place in the near future. Aeronautics Group systems are designed in light of those requirements.

It is our assumption that more and more users will take advantage of the drone platform in order to reduce operational risk and budget. The potential users are looking for a reliable, easy to use and maintain platforms. In addition, a very common request is for platforms that enable heavy lifting as well as long endurance, such as the Pegasus 120 that is the leading platform in the market for that aspect.

The Pegasus 120 is capable of lifting 45 kg and has the endurance up to 1 hour of flight. For example, think

about an electricity maintenance job that today is being done mostly by helicopters. The risk for the crew is extremely high as well as the cost and the productivity is low in respect to the Pegasus 120 capabilities. As the Pegasus 120 has fully autonomous flight capacities with a small logistic footprint enable to perform the same tasks with no risk, improving the productivity by 4 and reducing the cost by 10!

Additional advantage is the secured communication channel that prevent a cyberattack over the drone and in the radical scenario taking control over the platform and using it to crash into strategic asset.

Having said that, keep in mind that the Pegasus 120 is a platform that can take / integrate any payload for any task, you may use your imagination to understand the potential of such a platform. Below are few ideas that will describe better the Pegasus 120 potential.

Emergency situations such as volcanic eruption or earthquake, logistic support for food, drinking water, medical supply is always needed especially in territories with limited access. The Pegasus 120 will have no issue to support such need. A system with only 3 platforms is capable to deliver 1500 kg of supply per day.

In addition to the above, a fix wing platform such as the Orbiter 3 will enable to locate and recognize survivors and to guide rescue team to an accurate location. As an electro-optics missions seems to be obvious, advance payload such as cellular antenna, RF relay communication will provide an immediate solutions. The advantages of the orbiter 3 is a long endurance (up to 8 hours) using an efficient electric engine, it is runway independent thus, can take off and land in any terrains, easy to operate by a team of 3 persons and additional advantages.

One of the cure valves of Aeronautics Group is the customer – we implement this value into our solution by communality between the system thus it is very easy for an operator to operate all Aeronautics Group systems, in addition, the same control station is capable to control all Aeronautics Group drones. |

Five Steps to SAFER ORGANIZATIONS

A CHIEF OF POLICE ONCE ASKED FOR a completely safe laptop. He was given one but the security measures dictated that it could be only ever used in the safe room without the access to the public Internet. When he complained that the laptop is not usable for daily work he was explained that it is not absolute safety that he needs but safety measures and precautions according to the potential threat. In the era of big data, IoT and 5G it all comes down to simple equations of costs and benefits, potential risks and gains. There is no one magic solution to protect against falling victim to cyber crime but the risk can be seriously reduced by doing the following with your team, your processes and your behavior patterns.

First off map your business processes as well as supporting ICT infrastructure across the value stream, get to know the written regulations as well as the daily routine of the team. Also map the ICT services and infrastructure you use. Make sure you know what generates the value and where the resources come from, also how your data is stored and ICT processes managed. It is important to understand that the actual business process of your organization is not the one that is on the paper but the one that gets carried out daily. The same can sometimes apply to the ICT solutions. Evaluate the risks in the business processes and make sure your business is secure by design. Estimate the level of cost it takes and include it in the integrated cost model that unites the desired cyber hygiene and protection with the cost of service.

Secondly map the team and their roles as process owners and internal service providers to the potential information assets and data they hold. Pay attention that the level of one's position is not equal to the knowledge they may hold and that cyber attacks can be aimed at supporting other potential crimes or frauds. Build your privacy and human resources ICT policy around that information as well as general minimal level of cyber hygiene your wish to achieve. Make sure that everyone in your team know their role in the organization, in the generation of value as well as the responsibility they hold and how their actions affect the organization.

Third evaluate your cost model. Take into consideration all technical, procedural as well as behavioral changes you want to achieve as well as how it affects the service attributes. Look at the potential loss from falling victim to cyber crime including direct, indirect and publicity costs. Make sure that the gain remains greater than the cost and the residual risk within tolerated margins. Usually a minor change in processes or policies can reduce the cost up to 80 %. Plan the change carefully and holistically including the business processes across the value stream, HR policies, ICT policies and internal procedures, vendor and customer related processes.

Fourth carry out the necessary changes by starting with the business process. Then provide motivation as well as training to your team. Make sure they understand and follow the new process. Provide techniques and solutions to monitor the change.

Fifth step is the trickiest as you have to continuously monitor that the transformation you achieved remains and that the organization keeps evolving and carrying out improvements in the process of your organization and in the mindsets of your team.

Finesto Advisors is a team of security and business development professionals with their background in public as well as private sector. They bring together the collective knowledge of large public organizations, international corporations as well as small agile startups. Together they can provide you support business process design, business modeling, cost modeling as well as change mapping and roadmap development for making your business secure by design.

Thea Sogenbits is a security by design, business process security, and change management expert with her background in the education industry, IBM and International Association of Privacy Professionals. |



Thea Sogenbits

” One of the cure valves of Aeronautics Group is the customer

AUTONOMOUS AND SECURE DRONE SWARMING – WHAT IS NEEDED?

text: Arimo Koivisto, XXLSEC



CURRENTLY AVAILABLE commercial UAV airframes are capable and price efficiency for various tasks in commercial and industrial applications. They are even usable in public safety and defense applications to some extent – but they lack some required security and resilience features in this field. The problem is how to secure the sensitive data which the drones deliver.

TOWARDS SMART AND LEARNING SWARMS

Currently there is no suitable technologies which enable authenticated and secured autonomous swarms. There is need for distributed and shared computing between all nodes in the swarm. Adding AI to drones enables also swarms to do independent real time joint decisions with ‘no-leader’ model.

Swarms must be able to both react and learn from internal and external impacted events in the swarm or do autonomously tasks and requests. An example - one drone in swarm is hit by obstacle or jamming and other drones learn immediately this specific drone is not anymore available as swarm member and rest of the drones can also avoid this incident area to avoid same hit.

This kind of smart swarming requires that information between drones is real time, shared, authenticated and secured with MESH-topology networking – no room for centralized ground level computing and limited data transfer channels.

LEGACY TECHNOLOGIES ARE NOT ENOUGH

Encrypted real time communication between drones is not possible with current IP security protocols and transport methods. Actually current legacy IP protocol stack is 40

years old and not designed to do scaling of connections, multi-party authentication and security which are the modern requirements to enable smart swarms.

Typically a drone or UAV can carry many sensors and one problem is how to deliver the sensor information with secured and resilient methods. Current technologies allow one payload tunnel from flight control point to drones – this creates a choke point. Another problem is that this tunnel has limited capacity deliver the data.

Multivendor airframe turbulence creates also concerns and regulatory framework requires more detailed control over used sensitive communication, protocols and algorithms when handling classified sensory data from drones and UAVs. This need is in place because the information UAVs produce or sensory they integrate are often classified.

Data is always property of the user – not property of the platform or airframe manufacturer – so securing and separating payload data from flight control data channels is important, often mandatory.

DATA RAIN SOLUTION FOR DRONE SWARMING AND SECURE PAYLOAD TRANSFER

Data Rain system is XXLSEC developed solution which allows usage of COTS airframes, while keeping sensory integration and payload delivery under full own control and security model.

Data Rain system can be extended with Swarm Cipher Units, which creates volume benefits of multiple operating entities together with communication security, multi-party consensus and resource management.

This swarming technology is more than just ‘follow the

leader’ model where industry is currently focused on and Data Rain creates value to payload data management and swarm resourcing applications.

SENSORY & PAYLOAD – PRIVATE AND NATIONAL ASSET

DATA RAIN system implements *payload delivery, encryption and swarm resource management* between sensory sources and users requiring this information. Delivering drone produced sensory data to user in timely manner (and with required volume) often creates pressure to remove drone flight control post as choke point from implementation. Data Rain system does exactly this, making it possible for user at the ground to subscribe sensory feed directly from over head drones and even manage required sensory capacity in smart drone swarms. Data Rain Swarm Cipher Units enables also smart swarming and any-to-any secured and real time connectivity – a smart swarm.

Data Rain system is usable with all major IP networks and transmission channels. Swarm Cipher Unit implements multi-party security model to drone swarms and benefits from MESH technology in information delivery. Other networks like public or private LTE/5G nodes can be utilized as well, even they often create management overhead in infrastructure form.

Data Rain units in drones can ‘rain down’ data feeds from sensor equipment to user or user can up-link data feed from ground segment. Lifting data from ground to drone allows swarm cipher units to route this data inside swarm and get it’s routed down beyond operational horizon. This keeps information sources and destinations separated and secured.

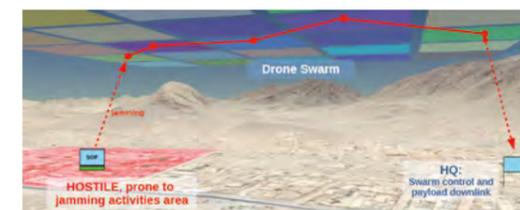


Image 1: Drone swarm is much more immune to jamming counter measures than traditional single drone operations.

This same model makes Swarm Cipher unit equipped drone swarms immune to ground originated jamming, because control happens inside swarm and possible down link beyond jamming area.

SENSORY PAYLOAD – VOLUME WITH SWARMING

Traditional single drone approach makes user to select equipped payload for single airframe and same time control and payload down link technologies become a choke point for operations.



Image 2: Traditional single drone approach enables one limited data tunnel and one UAV carries several sensors or other payload.

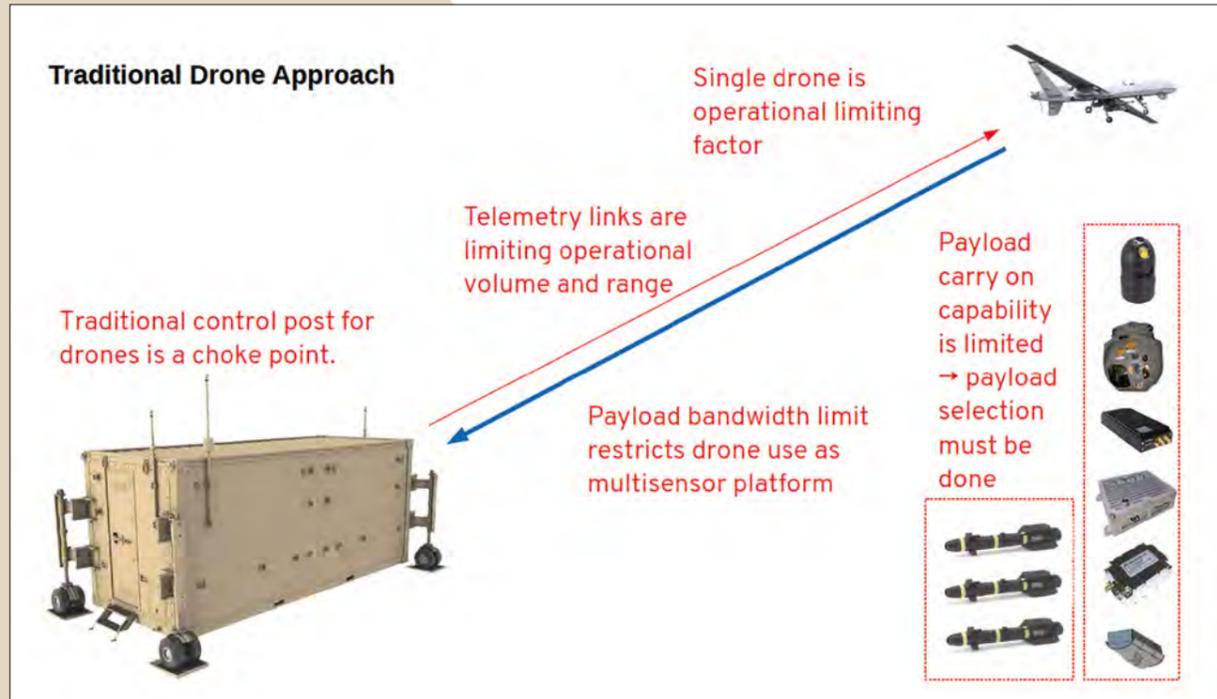


Image 3.1: In traditional drone approach, the telemetry link is a choke point and payload selection is limited.

Image 3.2: Drone swarm with increased and high volume distributed payload capability. Data Rain enables same payload shared to several drones - a swarm of drones replacing one heavy UAV with shared sensor and payload

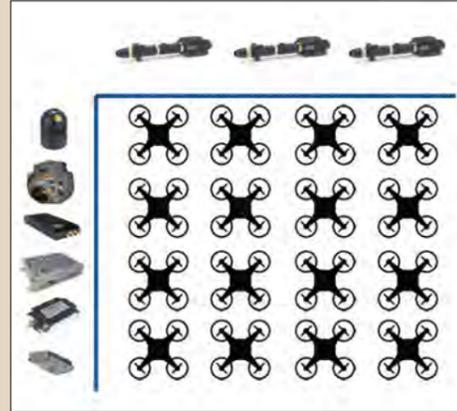


Image 4: Swarm Cipher Unit (SCU) enables shared consensus information tables between all drones and ground users #1 and #2.

SWARM Resources table

ID	GRID	PAYLOAD	TIME LEFT	CONSUMER	CLEARANCE
#1	X_1, Y_1	S_1, S_2	>8 h	#1	NFOR
#2	X_2, Y_2	S_1, S_2	<2 h	-	NFOR
#3	X_3, Y_3	S_1, S_2	<2 h	-	NFOR
#4	X_4, Y_4	K_1, K_2, K_3, K_4	>8 h	-	NFOR
#5	X_5, Y_5	S_1, S_2	>8 h	-	NFOR

CONSUMER Status table

ID	GRID	SENSORY IN USE	PRIORITY	CLEARANCE
#1	X_1, Y_1	S_2	2	NFOR
#2	X_2, Y_2		1	TS

With swarming, user can distribute the payload to several drones and make it possible to have more rapid incident reaction and payload capacity – rather than relying single drone approach.

SENSORY PAYLOAD - SWARM RESOURCING - MORE IMMEDIATE RESPONSE

Swarm Cipher Unit is XXLSEC developed unit which makes possible to form multi-party consensus between drone swarm members and ground based 'consumers' of payload data. This consensus is utilized to manage payload clearances, operation times and serving grid for each swarm member.

Drone tasking, optimizing radio resources and deliver required payload stream to users is one of the main tasks for IDC – Multi-party Consensus Protocol, developed by XXLSEC Ltd. The Swarm Cipher Unit is utilizing IDC protocol to enable smart swarming.

This means users #1 and #2 (image 4) at ground level can request specific sensor data from drone swarm independently and the swarm will deliver the information fast and secured - without the single data transfer link choke point problem.

IMMUNITY IN THE SKY

With this technology approach, offensive swarming is one potential development direction and swarm cipher units equipped with IDC protocol makes it possible to reach 'immunity in the sky' regarding counter activities against swarms.

Swarm controls the swarm, intelligence in body – with IDC protocol delivered multi-party consensus everyone in swarm is in equal position to take role or act in swarm. There is no single leader or leaders – the decisions are made in the swarm, between all units, even if the swarm has suffered losses.

SUMMARY

Drone swarming is not possible with current legacy IP security and authentication technologies. Multi-party computation capable technologies, like IDC protocol, combined with high speed MESH topology networking makes autonomous and smart swarming possible. Not only with drones but all connected systems like IoT sensor swarms, cloud computer swarms, autonomous connected vehicle swarms etc. Current needs for scalable and secured any-to-any connectivity can not be fulfilled with legacy technologies.

Image 4: Data Rain means securely delivered payload directly to user at the ground level. UAV control post is not anymore the choke point and payload information is separated from control post telemetry link.

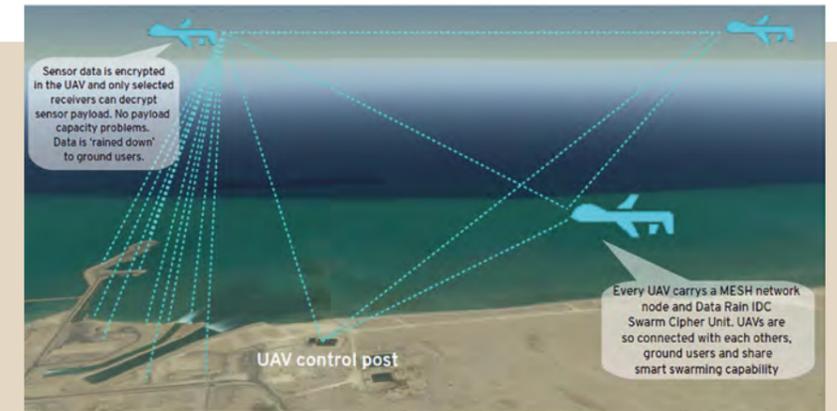
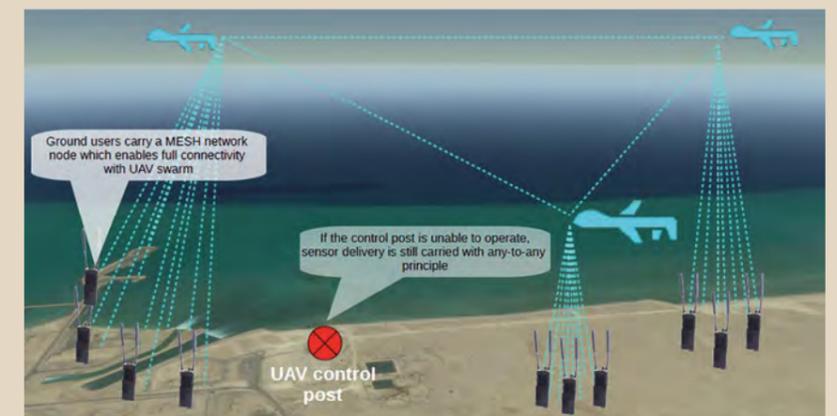


Image 5: In Data Rain solution, control post is not anymore a limit the operations. UAVs are able to carry missions even independently.



Cyberwatch Finland

➤ Offers You the acknowledged and trusted Finnish Cyber Security Intelligence, a comprehensive world-class solution for the needs of your entire organisation. We construct and help You to implement the appropriate cyber security strategies and to understand a holistic view of the cyber world and hybrid threats.

A unique impartial actor providing cyber security from strategic level to deployment models, recognising the scale of the required actions, Finnish well-known cyber expertise combined with educational competence in an online learning environment

We'll guide You to find the crucial investment targets to block the most critical vulnerabilities.



STRATEGIES AND ACTION PLANS

We provide cyber security strategies and their facilitation state-level operations, private sectors and international organizations based on a holistic view of the cyber world and hybrid threats.

With versatile management experience as well as expertise derived from the public and private sectors, we offer strategic action plans and their implementation for businesses and organisations.



CONSULTATION AND COACHING

Cyberwatch Finland provides professional and tailored situational awareness and strategic consulting, coaching and counseling for various aspects of comprehensive security. Counseling is offered for the leaders both at the private and government sector, with the goal in mind to bring true value to decision making and make investing in cyber security profitable. We provide most effective application of cyber security strategies and policies.

Cyberwatch Finland provides broad spectrum cyber security lectures and presentations going into greater detail on your chosen topic.



MONTHLY AND QUARTERLY REVIEWS

Our reviews offer compact analyses of the most significant cyber incidents in cyberspace, bringing forth an extensive view of the background, cause and effect of each incident. Trends as well as security breaches, vulnerabilities and cyber attacks are analysed through the lens of their relative impact and importance to today's organizations.



THEME REPORTS

A Cyberwatch Theme Report provides deep analysis of a specific theme, business sector or topic of importance. Theme Reports can be ordered on a case-by-case basis and updated as required.



EDUCATION

Cyberwatch Finland offers tailored cyber security training programs, comprehensive supervised learning sessions and e-learning courses for your executives and employees.

The aim of our thread-based training is to facilitate learning and raise awareness of cyber security and hybrid threats at all levels of your organization.

Our courses strengthen the ability of companies and organizations to recover from cyber attacks.



WORKSHOPS, SEMINARS AND GAMES

We offer custom workshops and seminars based on modern learning methods to understand how their cyber security strategies, teams and programs can be improved and raised to a higher level. Our seminars focus on cyber trends, incidents and emerging themes, conveying the latest knowledge on issues on cyber security trends by utilising modern learning methods and tools of analysis. Cyberwatch Finland's training – style games challenge your knowledge of cyber defense and test your organisational capacity during simulated security breaches and attacks.



CYBERWATCH TV

Cyberwatch Finland provides an Internet TV channel with topical interviews, discussions on cyber security and hybrid threats and live TV broadcasts of important issues of cyber security.



CONTACT US

Cyberwatch Oy, Eteläranta 10
00130 Helsinki, Finland

Aapo Cederberg, CEO
+358 40 024 6746
aapo.cederberg@cyberwatch.fi

Kim Waltzer, Chief Analyst
+358 40 771 4737
kim.waltzer@cyberwatch.fi





GOF U-space project demonstrates the future of Drone Traffic Management in Finland and Estonia during 2019

On 24 May the European Commission adopted European Union drone rules “to ensure increasing drone traffic across Europe is safe and secure for people on the ground and in the air.” The rules will apply to all operators of drones – both professionals and those flying drones for leisure. These new, binding rules will come into force starting 2020 in all EU Member States and include three of the first U-space services: registration and identification of drones and drone pilots as well as easily accessible information about the airspace.

text: GOF U-space

U-SPACE IS A SET OF NEW services relying on a high level of digitalisation and automation of functions and specific procedures designed to support safe, efficient and secure access to airspace for large numbers of drones. However, U-space is not only about drones. Today, airline traffic in Europe is heavily congested and the current air traffic solutions do not scale to larger traffic volumes or scale to more energy efficient routes. So, both manned and unmanned aviation have challenges that require us to embrace digital tools.

GOF U-space, which is named for the Gulf of Finland stretch of water that divides Finland from Estonia, is a SESAR (Single European Sky ATM Research Joint Undertaking) co-funded demonstration project taking concrete steps towards showcasing how U-space can serve both unmanned and manned aviation from the very beginning of its rollout. To get all required systems to interact, the GOF consortium is building a flight information management system (FIMS) with an architecture capable of integrating existing commercial-off-the-shelf Unmanned Traffic Management (UTM) components. The capabilities of the FIMS will be demonstrated in seven flying trials representing the most typical visual line of sight (VLOS) and beyond visual line of sight (BVLOS) missions.

The seven ambitious trials include ten drone operators in addition to manned aircraft: International parcel delivery between Helsinki and Tallinn, dense urban drone fleet operations in Helsinki with Police intervention and also in Tallinn in controlled airspace, 100km+ BVLOS multisensory inspection flights in forestry and utility inspection, co-operation with general aviation and recreational users at uncontrolled airfield, maritime search-and-rescue with drones and helicopters, and a world-first manned Drone Taxi flight from Helsinki-Vantaa airport to Helsinki.

The broad consortium with 19 members, includes three world-leading Unmanned Traffic Management (UTM) technology vendors Altitude Angel, Airmap and Unify, Air Navigation Service Providers Estonian ANS and ANS Finland and Frequentis with long experience from Air Traffic Management. Robots Expert coordinates live trials involving several drone manufacturers and operators Avartek, BVdrone, Cafatech, Fleetonomy, Hepta Airborne, Threod, and VideoDrone. The Finnish Air Rescue Society and Volocopter contribute with manned flights. Police authorities

from both countries as well as the communication authority TrafiCom in Finland participate to better understand the capabilities and requirements of modern drone systems.

The pace and stakes associated with digitizing aviation mean that huge development steps need to be taken, not just in managing air-risk, but also addressing ground-risk in the context of urban air mobility. Drones have exacerbated the need to come up with better ways of managing air traffic also in uncontrolled airspace and in cities to ensure that aviation’s amazing safety record can be maintained.

In a more practical sense, this kind of digitalization ties into why we need to ensure from the very beginning that U-space addresses all aviation stakeholders because it’s ultimately about being able to effectively share and safely utilize the whole airspace. Rescue helicopters, state aviation, drones, and soon general aviation all need to operate in the same airspace. We need to start to consider aircraft as being part of an aviation IoT, or Internet of Aircraft solution, be they manned or unmanned.

ABOUT SESAR

As the technological pillar of the Single European Sky initiative, SESAR aims to modernise and harmonise air traffic management in Europe. The SESAR Joint Undertaking (SESAR JU) was established in 2007 as a public-private partnership to support this endeavour. It does so by pooling the knowledge and resources of the entire ATM community in order to define, research, develop and validate innovative technological and operational solutions. The SESAR JU is also responsible for the execution of the European ATM Master Plan which defines the EU priorities for R&D and implementation. Founded by the European Union and Eurocontrol, the SESAR JU has 19 members, who together with their partners and affiliate associations will represent over 100 companies working in Europe and beyond. The SESAR JU also works closely with staff associations, regulators, airport operators and the scientific community.

ABOUT LENNULIIKLUSTEENINDUSE AS (EANS)

Estonian Air Navigation Services (EANS, Lennuliiklusteeninduse Aktsiaselts) is efficiently operating public limited company acting under private law, which provides Air Navigation Services in Tallinn FIR and at Tallinn and Tartu aerodromes. The Company has a long and fruitful experience in the modernisation of Air Traffic Management (ATM) and Aeronautical



”

Estonian Police and Border Guard Board has trained one hundred officers as Droneoperators who can use Drones on different cases.



FREQUENTIS

Information Management (AIM) systems, airspace organisation and procedures design and implementation. EANS has experience in the realisation of EU funded development and implementation projects. In year 2013 new PRNAV/CDA procedures were implemented in Tallinn TMA and Sherpa project were successfully finalised- building capacity for SBAS LPV procedures design and implementation, ASM Tool as well as DLS service implementation. In 2012-2014 we worked on IDSG IDP implementation projects. EANS participates actively in different kinds of regional initiatives, i.e. Northern-European FAB implementation projects, in the projects of Borealis ANSPs alliance, particularly expanding the recently implemented NEFAB FRA into NEFRA and Borealis FRA initiatives.

ABOUT ANS FINLAND

ANS Finland is responsible for managing the use of Finnish airspace as well as providing air traffic control services at airports in Finland. En-route services include area control services in Finland, airspace management, aeronautical search and rescue and air traffic flow management. Our technological air navigation services maintains and develops all navigation, communication, surveillance and monitoring systems related to en-route services, such as the air traffic control and radar systems required for flight surveillance. Our customers include airports, the commercial aviation industry, the Finnish state's aviation operations and military aviation, general aviation and pilot training schools.



AIRMAP

ABOUT ROBOTS EXPERT

Robots.Expert (REX) is a European consultancy focused on unmanned aviation. REX helps companies to adopt drone technology in their business, often combined with live demonstrations to jump-start the understanding of both the potential and of the challenges involved. Robots.expert's roots are in Finland with a strong network of drone stakeholders in Europe ranging from regulators to drone companies. REX's personnel have a strong background in UAS, technology and strategy, as well as in project management to support the tasks of facilitating demonstrations and to manage large projects or consortia.

Robots.expert also works with the foundation pillars of scalable drone business: U-space/UTM, telecommunications and precision weather. Examples of this is REX's involvement in SESAR's GOF USPACE -demonstration and in 5GDRONES on the use of 5G networks to support drones. In addition, REX works to establish drone rules and shared infrastructure in cities to promote the safe introduction of drones in the cityscape ensuring public acceptance. REX is the ambassador in Finland for EIP-SCC Urban Air Mobility. < www.robots.expert



ROBOTS EXPERT

ABOUT FREQUENTIS

Frequentis is an international supplier of communication and information systems for control centres with safety-critical tasks. These control centre solutions are developed and distributed by Frequentis in the business segments Air Traffic Management (civil and military air traffic control, and air defence) and Public Safety & Transport (police, fire and rescue services, emergency medical services, vessel traffic and railways). Frequentis maintains a worldwide network of subsidiaries and local representatives in more than fifty countries. The company's products and solutions are behind more than 25,000 operator positions in almost 140 countries. With this extensive portfolio, Frequentis is the leading provider of voice communication systems... all making our world a safer place every day! For more information, please visit www.frequentis.com

ABOUT ALTITUDE ANGEL LIMITED

Altitude Angel is an aviation technology company delivering solutions that enable the safer integration and use of fully automated drones into airspace. Through its Airspace Management Operating System, GuardianUTM, they deliver the essential software 'building-blocks' that enable national deployments of U-space compatible services. One of Altitude Angel's core objectives is to accelerate the development of drone-related solutions by building and maintaining the many complex 'backend' services. These services provide the data, storage, identity and command & control structures required to deliver excellent experiences to users via on-board drone solutions and mobile applications. In synchronicity with changing global drone regulations, Altitude Angel has already built a number of key services focused on delivering our long-term vision: fully autonomous, safe control of drones. Altitude Angel's leadership team has a wealth of experience across technology industry, specialising in building massively scalable, secure and distributed cloud based services, and a passion for aviation.

ABOUT AIRMAP DEUTSCHLAND GMBH

AirMap is the world's leading airspace management platform for Unmanned Aircraft Systems (UAS), commonly known as drones. AirMap partners with civil aviation authorities, air navigation service providers, drone manufacturers and solutions developers, and enterprises to integrate drones safely into the airspace. Developed by experts in aviation, airspace management, drone technology, mobile network communication, automotive and policy, the AirMap UTM platform includes solutions for registry, geo-awareness, notification, authorization, and traffic deconfliction to support autonomous, BVLOS operations. AirMap UTM has been deployed worldwide, including Switzerland, Czech Republic, the United States, and Japan. Visit www.airmap.com for more information.

ABOUT AVARTEK

Avartek is a Limited Partnership company founded in 1996 in Finland. Avartek ky is based on Avaruustekniikka ky which has provided target drones for the Finnish Armed Forces since 1968. We have serviced and trained our customers since those days and manufactured and sold over 1000 UAVs. We develop and manufacture unmanned aerial systems for long range heavy duty use. Our unmanned systems are economical, easy to use and extremely durable. Our systems are designed to accommodate multiple sensors and to handle day in day out missions in very challenging conditions. Our systems are based on 50 years of military target drone experience. Our drones are used in extreme military conditions and in challenging weather conditions. Our experience is unique and makes the core of our offering.

ABOUT BVDRONE

BVdrone is a BVLOS all-weather drone operator. BVdrone provides long-range, long-endurance operations for monitoring, remote sensing and surveillance missions, to create a new market for aerial work by lowering the cost, as well as provide services in conditions that civil, nonstate aviation normally does not operate in. BVdrone partners with other companies for sensor solutions and data processing. BVdrone is based in Finland.

ABOUT CAFA TECHNOLOGY

CAFA (Center of Automated Flights Applications) develops 3D maps for automated drone flights. CAFA 3D maps visualize drone flights in the true 3D environment. CAFA has developed a Tallinn 3D Map and its web application for drone operations (<https://cafa3d.com/3dpoc>). CAFA 3D map has also Google Earth 3D cities integration for planning low altitude drone operations in Europe and in USA. 3D Map is essential part of safe and efficient drone route and flight corridor planning.

ABOUT ESTONIAN POLICE AND BORDER GUARD BOARD (PPA)

Estonian Police and Border Guard Board is responsible for public order and general safety in Estonia. Estonian Police has been developing its capabilities to control public order by using Drones. Estonian Police and Border Guard Board has trained one hundred officers as Droneoperators who can use Drones on different cases (public events, security measures, search of lost people, boarder surveillance, technical crime investigation support and traffic accidents). Situation Pictures of flying objects is crucial part of possible counter measures. Estonian Police and Border Guard Board contributes to the project by organizing demos and testing different circumstances.



CAFA 3D

ABOUT FINNISH COMMUNICATIONS REGULATORY AUTHORITY (FICORA)

FICORA is the regulator of spectrum, cyber security and communication markets in Finland. The authority's activities contribute to a reliable information society and secure the status and rights of users of communications services by ensuring that society, business and citizens have access to, for example fast and reliable telecommunications connections, effective communications markets, efficiently-used radio frequencies, numbers and codes, reasonablypriced communications services of good quality, versatile electronic media services, and objective information on the development, pricing and service level of communications markets and services. FICORA maintains an overview of the functionality of electronic communications networks and information security, and reports of eventual information security threats. One of FICORA's key performance targets is to support Finland in becoming the 5G technology leader and thereby ensure access to advanced electronic services for every member of society. FICORA functions under the Ministry of Transport and Communications Finland. Read more: <https://www.viestintavirasto.fi/en/index.html>



MINISTRY OF TRANSPORT AND COMMUNICATIONS FINLAND

ABOUT THE FINNISH AIR RESCUE SOCIETY

The Finnish Air Rescue Society (SLPS) has 38 affiliate members, which will provide the actual aircraft and manpower to the project (test flights with general aviation aircraft, coordinated by SLPS). The Air Rescue Society is one of three coordination Societies of the Finnish Voluntary Rescue Service, a force of almost 20 000 voluntary persons, and is responsible of all Aviation operations of the Service. The Society maintains 35 readiness groups, with one 24/7 duty officer at the time to forward different flight operations asked by the Police and Fire Departments.



”

Finland in becoming the 5G technology leader and thereby ensure access to advanced electronic services for every member of society.

ABOUT FLEETONOMY.AI OY

Fleetonomy.ai Oy develops a remote operating platform for automated vehicle fleets for vehicle fleet operators. Platform manages key issues in the automated vehicle operator environment including regulation, exception and responsibility management while keeping the human in the loop. Foundations rest upon innovations in interactive 3D control systems for display and analytics of complex data sets for managing fleets of automated vehicles and airborne drones.

ABOUT HELSINKI POLICE DEPARTMENT

There are tens of trained officers as Drone-operators in Helsinki Police. Helsinki PD has approximately ten drones for operative purposes 24/7. They are in use almost every day - especially in public events, security measures, searching lost people, barricade situations, supporting technical crime investigations etc. for three years now.

ABOUT HEPTA AIRBORNE

Hepta Airborne, a leading robotics and Big Data company, has developed the next generation power line inspection technology. The technology consists of in-housed developed 6 hour long-durance UAV, upgraded measurement sensors and autonomous post-flight data analysis platform. The whole system inspects hundreds of kilometres autonomously and analyses the collected data. Utilities and Network operators receive a detailed overview of their assets, automated defect reports and detailed vegetation analysis.

ABOUT THREOD SYSTEMS

Threod Systems specializes in developing, producing, and operating Unmanned Aircraft Systems (UAS) that are designed for information collection and exploitation in military, governmental and civil applications. Threod supports the decision-making process on every level of command. Threod Systems is known for rapid product development and tailor made UAS solutions for small multirotors, fixed-wing UAV platforms, and in-house developed subsystems. Threod System designs, develops, manufactures and operates Unmanned Aircraft Systems and subsystems for information collection, surveillance and other tasks related to unmanned sensing including VLOS and BVLOS operations.

ABOUT UNIFLY

Unify is the leading Unmanned Traffic Management software developer, deploying the new unmanned ecosystem on a national scale in four countries. Since the foundation of the company, Unify continuously works on upgrading this system according the U-Space blueprint. Due to the step-by-step approach, Unify can easily integrate legislation and airspace for specific countries and stakeholders. Since 2015, Unify participates in Horizon2020 projects, targeting specific requirements of the Unmanned Traffic Management system.

ABOUT VIDEODRONE

VideoDrone Finland Oy has designed and manufactured multicopters for professional applications since 2011 and as a limited liability company since 2013. The drones are completely designed, manufactured and tested by our experts. Our drones are used currently for various technical inspections, land survey and planning, orthoimaging and point cloud processing, oil and other environmental accidents, accident investigation and surveillance. Our customer base includes land surveying professionals, companies, municipalities, educational institutions and farmers. VideoDrone delivery is always a complete, tested and ready-to-fly package to help the customers together with the operational training.

ABOUT VOLOCOPTER

Volocopter is developing autonomous air taxi services, to supplement public transportation in large cities. Their Mobility as a service solution will be sustainable, quiet, and time efficient. The Volocopter resembles a helicopter but is based on drone technology, it is electrically powered, and much safer due to multiple redundancy in all flight critical systems. As true pioneers, Volocopter has been flying regularly since 2011, both piloted and autonomously. The first commercial routes are planned to be up and running by in 2022. |

THE FLY-BY GUYS

The AI in the Sky

The Fly-by Guys are working with GoodVision, an artificial intelligence and deep learning platform. Both parties will work together to increase the deployment of smart city technology across Finland and the Nordics.

The municipality's ability to quickly respond to emerging needs is extremely limited by existing data collection and evaluation techniques... until now.

The ultimate intent is for cities to be able to leverage unstructured video data, uploaded into the analytics platform and result in making more informed and data driven planning, funding and project development decisions. The Fly-by Guys have spent a significant amount of time looking at how best to leverage 'eyes in the sky' drone footage with best in class AI capabilities, of which we found GoodVision to be the leader in the field.

Both companies believe that with advances in sensor technology and computing capacity, there is a significant opportunity to understand infrastructure performance in near real-time and to respond to any questions on transportation issues with much more detail than in the past, at a much faster rate, and in a cost-effective manner.

The partnership allows the Fly-by Guys to exclusively resell GoodVision to clients and enable faster market adoption of the technology. There has already been a high interest from cities and municipalities across Finland looking to trial this technology.

For further information about The Fly-by Guys & GoodVision, please contact stephen@flybyguy.fi



The Fly-by Guys

CYBERWATCH FINLAND REVIEW



5G – MORE EFFECTIVE ESPIONAGE OR BETTER NATIONAL SECURITY?

➤ There is ongoing speculation on the security of 5G networks and the purpose of their suppliers. Accusations against the Chinese, especially Huawei, have been most prominent. The effects are already evident in Huawei's sales.

The question is, first and foremost, about trust. Trust must exist in technology, manufacturers, service providers, companies, states, individual persons or groups with different motives. It's inevitably about who has access to the system or the opportunity to operate the data at different stages. **Safety is always about the reliability of the whole ecosystem.**

Overall it is about fighting for dominance over all networks and, if necessary, taking advantage of information provided by these networks for various states' political and military purposes, as well as for commercial purposes. Alongside the Internet and the globalisation of digital services, there is now an attempt to restore the borders of states and the control associated with them.

The ongoing speculation on network device security is a combination of many security issues of different levels, with emphasis placed on collaboration and the ecosystem.

The change towards the 5G world will require active sharing of information, the review of the boundaries of authoritarian control and the wider dialogue between the participants. It is difficult to build real cooperation without mutual trust.

Network equipment suppliers refrain from commenting on each other's shortcomings or reliability, allegedly due to the fear of being targeted by competitors and the media. An exception is an interview with Nokia's Chief Technology Officer Marcus Weldon, who warned Britain of the security flaws in Chinese products. In his comments, Weldon referred to a report published by US-based company Finite State, which found significant shortcomings in Huawei products. Nokia resigned from its position as Chief Technology Officer and stressed that it did not represent the company's official position.

One reason for the silencing of network equipment suppliers by their competitors' products may be that they are familiar with the industry players and realities, such as political, economic, military and technical dimensions, and government intelligence requirements for the use of possible advantageous backdoors.

In a way, Huawei is undergoing a public global security audit. None of the other competitors would certainly want the same negative attention themselves.

The Finite State report places importance on many qualitative shortages in software development and their upgrade processes and calls for transparency in processes and teamwork. The most troubling is the discovery of software vulnerabilities that are found hidden in the code after being updated and repaired. These findings provide evidence of purposeful exploitation of vulnerabilities, although actual back doors did not appear in the studies. The issue is that various important and valid management features can in some cases be used as back doors.



The escalation of the national security debate around Huawei has caught a number of 5G enthusiasts off guard. The United States, Australia, New Zealand, Japan and the Czech Republic, among others, have imposed restrictions on the use of Huawei 5G solutions over national security concerns; much of Europe is pondering whether to follow suit. Summed up, the nations' worries are rooted in the ties between Chinese communications technology companies and its intelligence services, reinforced by China's political and legal environment requiring cooperation with intelligence agencies. Perceived or real, fears persist that adopting Huawei 5G technology will introduce a critical reliance on equipment that can potentially be controlled by the Chinese intelligence services and the military in peacetime and incrisis.

—NATO Cooperative Cyber Defence Centre of Excellence (CCDOE), 2019

The general decline distrust of digital services and companies, particularly at the political level, is wor-rying. For companies and service providers, this means a more conscious choice of partners and tech-nology. From the perspective of users, the choice is more about which manufacturer's smartphone is used and what information is made available to the applications. However, smartphones, apps, and social media services build the most significant profile of individuals, whether they like it or not. In order to reap the benefits of digitalization and effectively take advantage of IoT devices, we need an efficient and secure 5G network. For example, so-called smart cities and houses cannot be solely built on modern technology, so the development of cyber security and digitalization must go hand in hand.¹



Through analysis of hundreds of thousands of firmware im-ages, Finite State has found that, on average, more than 80% of software in a device is duplicated in other devices - illustrating just how interconnected software supply chains are.

CYBER SECURITY IN EUROPE: STRONGER REGULATION AND BETTER PROTECTION

The European Commission published guidelines and recommendations for Artificial Intelligence Applications.

In April, the European Commission published a preliminary version of the ethical guidelines for Artificial Intelligence Applications. The background to this work is the Commission's vision of supporting ethical, safe and most advanced artificial intelligence produced in Europe. The Commission's vision is based on threepillars:

- preparing for socio-economic change
- increasing public and private investment in artificial intelligence
- ensuring a proper ethical and legal framework to strengthen European values.

To support the attainment of artificial intelligence, the Commission set up an independent high-level expert group (AI HLEG) tasked with producing two documents: **ethical guidelines on artificial intelligence** and **policy and investment recommendations**. According to the published guidance, artificial intelligence must be **legal, ethical and sustainable**. The guide raises seven key points for developing and deploying reliable artificial intelligence:

- 1) Human activity and human control
- 2) Technical Reliability and safety
- 3) Privacy and data management
- 4) Transparency
- 5) Diversity, non-discrimination and justice
- 6) Social and ecological wellbeing and
- 7) Accountability.²

Ethical guidelines for the development of artificial intelligence are a welcome and important component. It is also an indication that the European Commission has addressed the potential effects of artificial intelligence and that strategic management has been put in place. The management will help address issues from different perspectives. On a global scale, the EU's pursuit of ethical artificial intelligence appears somewhat idealistic. It is likely that in the Global Artificial Intelligence race, EU's ethical values will be praised. In fact, open-mindedness and the artificial intelligence guidelines can be used against Europe. Artificial intelligence will be used for both good and bad - it remains to be seen who wins. Using artificial intelligence to automate cyberattacks and target analysis, for example, constantly challenges cyber security systems and the level of human education.

SANCTIONS TO PREVENT AND RESPOND TO CYBERATTACKS IN THE EU.

On 17 May 2019, the European Council established a framework that allows the EU to impose targeted restrictive measures to prevent and respond to cyberattacks that pose a significant external threat to the EU or its Member States.

The framework allows the EU, for the first time, to impose sanctions on individuals or communities responsible or involved in cyberattacks or their attempts. Sanctions may also be imposed on parties that support attacks, financially or technically, or on persons and communities associated with them. Restrictive measures include: a travel ban to the EU, and freezing of the assets of the individuals and communities. In addition, EU citizens and communities are banned from making funds available to sanctioned individuals.³

At the very least, using sanctions to prevent cyberattacks is a challenging task. The strong evidence obtained through intelligence and crime prevention, justifies the proactive measures taken to prevent attacks. Sanctions are designed to be proportionate to the cyberattack, its



threat or potential impact on a case-by-case basis. The deniability of cyber events and the uncertainty of anonymity are always present and bring forth important components to the justification and level of sanctions.

Sanctions against state officials are always accompanied by politics, which can complicate the decision to retaliate. Sanctions against certain parties can be of greater impact, and the victims can be complete strangers to the situation. For companies, sanctions increase the risk of becoming a political pawn. At the personal level, sanctions can provide a sufficient deterrent effect, increasing the fear of being caught. A travel ban on the EU or an asset freeze may in some cases work, but their effectiveness is uncertain. The freezing of funds is increasingly driving operations towards the use of cryptocurrencies and strong anonymity. The threat of sanctions is unlikely to affect the activities of governmental or organized cybercriminals.

THE EU CYBERSECURITY ACT ENTERED INTO FORCE ON 27 JUNE 2019.

The European Union Cyber Security Agency (ENISA) mandate was approved.

Under the Regulation, ENISA will carry out its tasks with the means to achieve a high common level of cyber security throughout the Union. Executed by actively supporting the Member States, the Union institutions and bodies in improving cyber security. ENISA shall provide consultation and expertise on cyber security to Union institutions, organizations and bodies and other relevant Union stakeholders.

A **European cyber security certification framework** will be set up to raise the level of cyber security in the Union and to standardize European cyber security certification systems at Union level. Thus, im- proving the capacity to create a digital internal market for ICT products, services andprocesses.

The stabilization of ENISA's role is an important message that indicates that cybersecurity is being invested in and that promoting cybersecurity is an essential part of the normal functioning of the Euro- pean Union. The aim is also to contribute to reducing the fragmenta- tion of the internalmarket.

The role of the European internal market and strong cooperation in developing cyber security is im- portant in the current geopolitical situation. The new European certification framework will improve the development and awareness of European cybersecurity products, services and software, both in Europe and internationally.⁴

DRONES ARE A NEW TOOL FOR CYBER-ATTACKS

The development of the unmanned aerial vehicles, or drones, has been fast and rather multidimensional. Initially it has been used to fulfill military needs, but the explosive increase in leisurely use has led to falling prices and rapid technological development. At the same time, it is noticeable that drones are useful for many civil societal tasks as well, such as surveillance tasks, logistical transport for agriculture, etc. It would be more appropriate to refer to autonomous devices as some of these tools do not fly but crawl, dive ordig.

It seems clear that drones are becoming a part of the critical infrastructure of modern societies, automatically becoming a potential target of cyberattacks. For example, their control systems are easy to capture, disrupt, or deceive with cyberattacks.

The 'security by design' principle has once again been forgotten. Security considerations are only beginning to emerge when, the scale of the change and how fast the capacity of modern autonomous devices will increase, are in question. The closure of Gatwick Airport in December 2018 was the first serious warning of the kinetic threat posed by drones. It was also a reminder of the need for regulation and the inability of the security authorities to respond appropriately to this type of new threat.

Drones have also been developed as a platform for cyberattacks. They can be used to conduct aggressive cyber surveillance, influence, and deception. You no longer have to drive a truck near the destination, for example, but the operation can be overseen with intelligent small drones. The users of drones vary from state operators and cyber-criminals to various activist groups.

This development is again a reminder of how valuable digital innovations can be abused and creating new security threats. In the future, we will definitely see new "drone operations" as part of the growing hybrid influencing. The development of autonomous devices must be taken into serious consideration in future cyber security development projects both as a threat and as an opportunity.

Military use is also increasing and evolving as a part of this civilian development path. The Iran-US incident in June is a living example of the importance of cyberattacks and drones as a part of military operations.⁵



THERE HAS BEEN NO SIGNIFICANT DEVELOPMENT IN THE SAFETY OF THE NETWORK EQUIPMENT FIRMWARE IN OVER 15 YEARS.

➤ According to a comprehensive study of the Security Ledger's 6000 network devices and their firmware 2003-2018 comprehensive study, there have been no developments in the security development of the firmware, despite the fact that the number of cyber-attacks is on the rise. Most of the devices have serious safety deficiencies and their safety features have hardly been developed over the years.⁶

Network devices and manufacturers are expected to take upon the "Security by Design" approach, which means designing hardware and software safe by default. This may not be the case. The development of network devices and firmware for pre-products can take several years and taking security into account in the hardware and software development increases production costs. If the hardware is intended for use in a "secure" intranet, it is better to assume that the device itself is not secure.

It is likely that the use of the term "security by design" will be seen more in the next few years. But whether it is just marketing, or actual safer products, remains to be seen.

THE SYSTEMS OF AN INDUSTRIAL COMPANY OPERATING IN MORE THAN 50 COUNTRIES WERE ATTACKED-INCLUDING SOME OF THE FACTORIES IN FINLAND

➤ The industrial mineral company Omya was subjected to an online attack, which resulted in the ceasing of operations as a precaution in all factories. The suspension also concerned three factories in Finland in Imatra, Kemi and Forby. Omya is an international company with a Swiss background and employs over 8,000 people. There are more than 175 factories worldwide, in more than 50 countries.⁷

Omya has been hesitant about reporting the attack, which leaves a lot of room for speculation. Cyber attacks on global mineral and commodity companies demonstrate the tangibility of the risks of the digital world in the physical world. The magnified effects on stakeholders and other industries can appear as threats to where a single vulnerability or cyber attack can lead to globally.

The company's ability to react, communicate and recover says a lot about both the ability of the company and the industry and their preparation for cyber threats. However, it can be assumed that attacks on large raw materials companies and production plants will increase in the coming years.

Recently there has been an increase in the so-called Big Game Hunting phenomenon⁸, in which attackers seek maximum economic benefits. In March 2019, the aluminium manufacturer Norsk Hydro was subjected to a ransomware program attack. The company did not pay the ransom, but the cost of the recovery from the attack rose to more than 52 million euro.⁹



BIOMETRIC IDENTIFICATION DATA FOR MORE THAN A MILLION PEOPLE ARE AVAILABLE FOR DOWNLOAD ONLINE

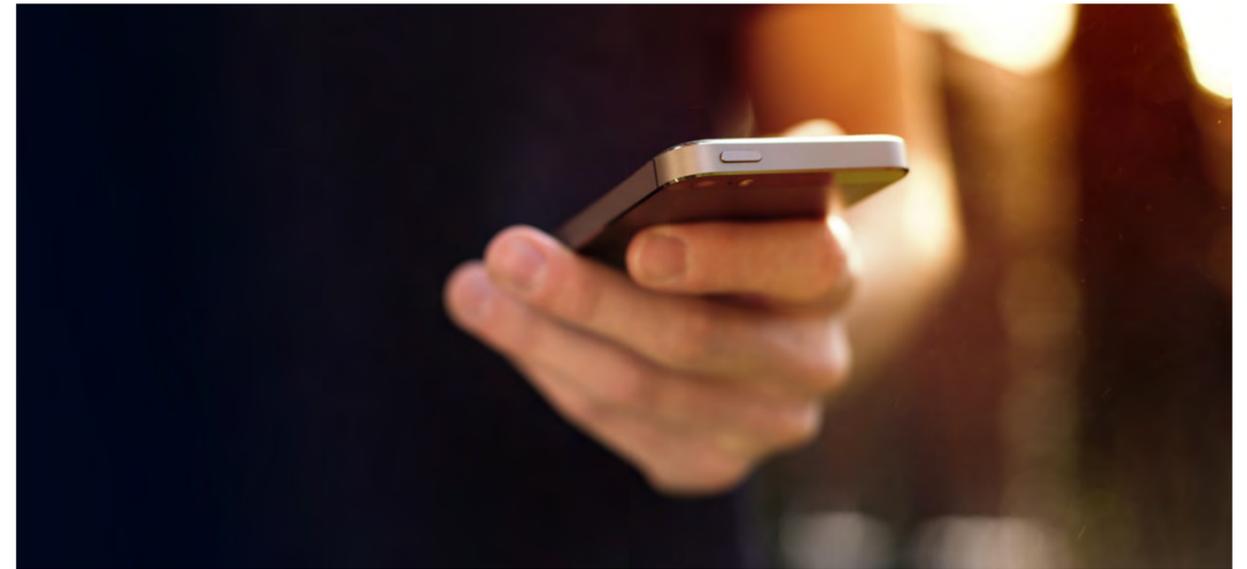
➤ The biometric identifiers, usernames, passwords and other private data of more than a million citizens were found in the Open Biostar 2 system database, partly from unsecured servers used by, among others, the British police, Major banking groups and companies providing security services.

Biostar 2 is a product of the Suprema company providing global biometrics and security services, an open web-based integration platform for user and access management.¹⁰ The vulnerability found was associated with the Biostar 2 Cloud integration interface.

The number of biometric identifiers is rising and its spread is encouraged by the use of biometric identification in smartphones, computers and various security checks. The challenge is the secure processing of bio-metric data in the service architecture and the so-called third parties that process data at different stages of the process.

The same challenge also applies to other technologies associated with automatic identification and the processing of related data. For example, in Xinjiang, China, in February, a data leak occurred in which the personal data of 2.6 million people from human face detection and GPS location databases were revealed in the public network completely unprotected.¹¹

Biometric data combined with automated facial, character, and voice recognition data leaks and abuse will increase as the services utilising them become more common. This should also be taken into account in matters relating to the use of genomics and health-related genetic analyses as well as the drafting of laws, both in Finland and abroad.



DUE TO SERIOUS VULNERABILITIES IN APPLE PHONES, ESPIONAGE HAS BEEN POSSIBLE FOR YEARS.

➤ Apple iPhone smartphones have found a number of serious vulnerabilities that enabled devices to be seized without user intervention by sending different message types (including iMessage, multimedia and SMS, Apple Mail email). At worst, the vulnerabilities have been known to hackers and state actors already for a couple of years.¹²



Apple released a patch update iOS 12.4, but at the same time it reopened a once-fixed vulnerability that could break iPhone security by installing a 'jailbreak' security modification. Jailbreak apps have their own risks, since potential applications are not verified anywhere and there is no information about their safety. The jailbreak version of the modern version of iOS has not been available for years, so Apple's mistake can be considered quite significant in this regard. Apple released an instant patch for iOS 12.4.1 about a week later.¹³

This is a bad blow for iPhone's reputation as a safe and hard-to-break smartphone. The case also shows that mistakes happen to everyone. It's about how quickly the errors are corrected and how the reputation risk is managed. With increasing cyber-attacks and vulnerabilities, the security and reliability of the software development process will be emphasised in the future. The question of responsibility will certainly be discussed for a long time.



It doesn't matter how good your crypto is if the program has bugs on the receiving end.

- NATALIE SILVANOVIICH,
GOOGLE PROJECT ZERO

BIBLIOGRAPHY:

- 1 <https://finitestate.io/finite-state-supply-chain-assessment/>
<https://www.theinquirer.net/inquirer/news/3078119/nokia-huawei-5g-spat>
<https://www.traficom.fi/fi/ajankohtaista/liikenne-ja-viestintavirasto-julkaisi-selvityksen-5gn-kyberturvallisuudesta>
- 2 <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines>
<https://ec.europa.eu/digital-single-market/en/news/eu-artificial-intelligence-ethics-checklist-ready-testing-new-policy-recommendations-are>
- 3 <https://www.consilium.europa.eu/fi/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/>
- 4 <https://www.reuters.com/article/us-eu-cyber/days-before-elections-eu-approves-new-cyber-sanctions-regime-idUSKCN1SN1FQ>
<https://www.consilium.europa.eu/fi/policies/cybersecurity/>
- 5 For good D. (2014). Meet Snoopy: The DIY drone that tracks your devices just about anywhere, 26 March 2014 Pritchard S. (2019). Drones are Quickly Becoming a Cybersecurity Nightmare, - Threatpost, 22 March 2019 <https://www.traficom.fi/fi/ajankohtaista/kansainvalisen-hankkeen-drone-kokeilut-kaynnistyneet-suomessahttps://www.eepelit.fi/ensimmaisest-drone-olympialaisest-suomessa-vauhdittavat-globaalia-kasvua/>
- 6 <https://securityledger.com/2019/08/huge-survey-of-firmware-finds-no-security-gains-in-15-years/amp/>
- 7 <https://www.tekniikkatalous.fi/uutiset/yli-50-maassa-toimivan-teollisuuyhtion-jarjestelmiin-hyokattiin-hs-myo-osa-suomen-tehtaista-pois-kaytosta/4fe587dd-fdfe-4b0e-9065-c8f962cde04d>
- 8 <https://www.wired.co.uk/article/norsk-hydro-cyber-attack>
- 9 <https://www.bbc.com/news/business-48661152>
- 10 <https://www.supremainc.com/en/platform/hybrid-security-platform-biostar-2.asp>
- 11 <https://www.ft.com/content/9ed9362e-31f7-11e9-bb0c-42459962a812>
- 12 <https://googleprojectzero.blogspot.com/2019/08/the-fully-remote-attack-surface-of.html>
- 13 https://www.vice.com/en_us/article/qvq77/hacker-releases-first-public-iphone-jailbreak-in-years

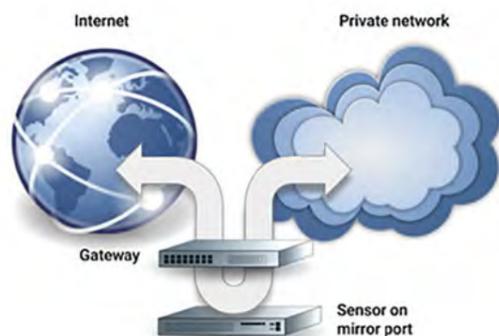
SENSOR ON THE EDGE

text: Sami Petäjäsoja



INTRODUCTION

Network sensors give you lightweight detection capabilities. In this article we discuss installation of sensors at the key network locations, typically at the edges. This configuration keeps installation and maintenance costs affordable and scales up easily. Edge deployment gives you visibility to the wild west of the Internet, while keeping your private network traffic out of the spotlight



Sensor deployed on the perimeter of private network

SENSORS ON THE EDGE

The deployment configuration for sensors depends on your objectives and the level of network access that is required for deploying the capabilities to meet those objectives. Placing a sensor at the edge of network primarily focuses on the metadata of network traffic with no visibility inside encrypted traffic. There are scenarios where you'll want to place sensors inside the perimeter, but let's live on the edge for now.

An edge configuration is a good alternative, for example, but not limited to, the following use cases:

- CERT or SoC teams responsible for coordinating the protection of national Critical Infrastructure (CI)
- Large organisations with multiple branch offices or networks looking to quickly deploy centralised security monitoring capabilities
- Anyone looking for a quick start on network security monitoring with minimal impact on existing infrastructure

BENEFITS ON THE EDGE

Sensors are installed in a transparent manner. This transparency works on two levels: Your own operations are not impeded by the sensors, and the would be attackers will have harder time detecting the presence of monitoring. Even if the attackers manage to disable log forwarding or host-based detection measures, the network traffic can still be inspected.

Network sensors are complementary to other forms of detection capabilities the organisation has. Captures of protocol metadata and contents provide rich alerts. To secure forensic data for the incident response, sensors can be kept at arms length from your IT systems. For example, you should not share single sign-on between sensors and your other servers. Sensors also offer additional context to alerts from other detection sources. Metadata volumes are low compared to overall data volume and can be stored for extended periods, even years. This data can then be utilised for threat hunting. However, in order to protect the privacy and comply to regulations, you should have explicit control over the data content, access and duration of the retention



Connecting threat intelligence with sensors provides additional context

There is an increasing amount of data available about compromised hosts and attacks. This data is called threat intelligence and it is available from both public and private feeds. If you're a receiver of threat intelligence, you can utilize metadata history to check if your organisation has been targeted or affected. In the cases where logging or endpoint protection falls short, network sensors are a stopgap measure for detection. Portions of the infrastructure can also remain unmonitored by other means due to technical reasons, and network monitoring reduces the resulting residual risk.

CAPABILITIES ON THE EDGE

So what are the monitoring capabilities edge deployment gives you? Implementations may vary, but in this paper we'll focus on Instruments in current version of SensorFleet sensor.

FULL PACKET CAPTURE

As the name implies, packet capture enables storage of full network traffic for auditing and forensics purposes. Stored traffic should be time indexed for filtering during the investigations. Filtering can then be done based on timestamps, ports or IP addresses. The sensor itself can typically store a few days of traffic. That's a broad statement on purpose, since traffic volumes and exact sensor model will set the hard limits. Another, storage capacity saving option for traffic capturing is storage that is triggered by alerts from one of the other instruments. This mode gives you a snapshot of traffic with time window before and after the alert.

The captured traffic can be protected at rest by encryption, should some nefarious individual walk away with your security device.

SURICATA IDS

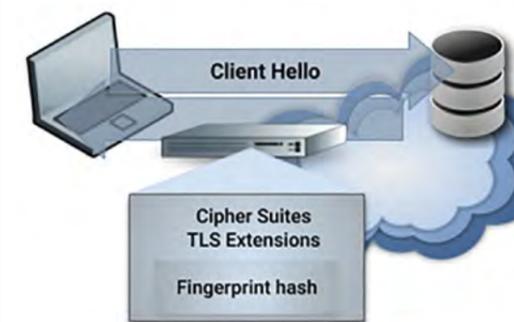
Suricata IDS packs a punch for signature based detection. Suricata is compatible with Snort rules, which enables use of widely shared Snort rulesets and threat intelligence that's shared in Snort format. For the complex detection scenarios, Suricata introduces an expressive native scripting language. High bandwidth requirements have been taken into the account with multi-threaded design from the beginning, making Suricata a good choice for edge sensors.



The benefit of identifying malware based on TLS or SSH fingerprint comes from the fact that while infrastructure indicators such as IP addresses or domains may change frequently, malware families have relatively static fingerprints.

Besides regular IDS detection, TLS and SSH fingerprinting is worth mentioning here as it's a technique we've seen good results with. TLS as a protocol has multiple configuration options and each client tends to have a unique fingerprint. Unexpected or known malware client profiles can be identified based on these fingerprints.

The benefit of identifying malware based on TLS or SSH fingerprint comes from the fact that while infrastructure indicators such as IP addresses or domains may change frequently, malware families have relatively static fingerprints. From a technical perspective, server side fingerprinting works in similar fashion, but is not as useful as the server space is dominated by a handful of implementations.



Fingerprinting TLS Clients with the Suricata IDS

BLACKLIST ALERTS

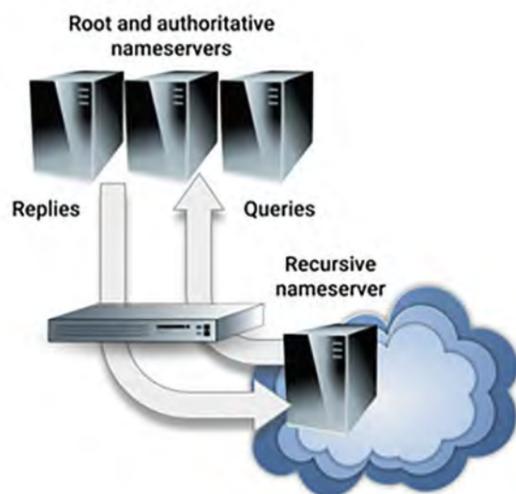
Blacklisting is a specific IDS use case, but separating it logically into its own dedicated component makes the management of blacklists easier. With blacklisting on the edge sensor, you're typically looking for malicious network identities such as domains or IP addresses. Alerts will be raised for both malicious identity trying to make inbound connection, or host inside the perimeter trying to make outbound connection to a malicious identity. Along with IDS, blacklists make up a good integration point if your organisation is receiving threat intelligence from third parties.

PASSIVE DNS

Despite having reached their terrible teenage years (first described by Florian Weimer in 2005), Passive DNS is among the underutilized gems of security monitoring. When integrated with an edge sensor, Passive DNS is well placed for building a database on DNS queries and responses. In the case of local name server, only cache misses are recorded, but luckily that's not detrimental to our intended purpose.

So what to do with the database of DNS queries and responses? Passive DNS database essentially gives you a mapping of domain names to IP addresses over time and you can use this information in different ways.

- Once certain domain name or IP address has been marked malicious, you can go back in time to see if these indicators of compromise are present in your DNS traffic history.
- Malware and phishing sites change their domain names frequently. With Passive DNS, you can set up alerting if a query for a new domain resolves to known bad IP address. Similarly, you can easily set up monitoring for DGA (Domain Generation Algorithm) domains used by some malware strains.



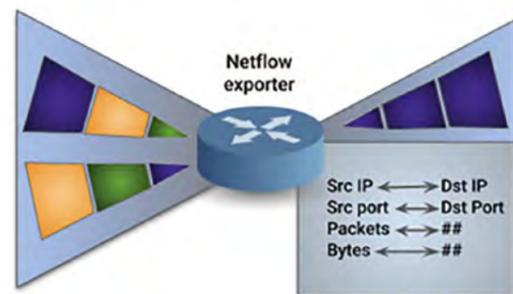
Passive DNS recording the cache misses

NETFLOW

NetFlow export and analysis for post-mortem inspection is a great addition to your sensing toolbox. NetFlow stores header information about a network flow and can be used to ask questions like "has anyone ever communicated with this IP?".

A concrete example for NetFlow usage in security analysis would be that a full packet capture has had its retention time expire just as new threat intelligence comes in. A security analyst or SoC team can use NetFlow to see if anyone in the protected network has communicated with suspect IP addresses in the past, which could indicate a compromise.

The advantages of NetFlow are compactness of stored data and exclusion of any payload information. The network level identities of internal network users and devices could be masked because of address translation (NAT) as the edge sensor typically sees only an edge device such as a proxy or a gateway as the source or destination of the traffic. The identities can be unmasked in investigations from the edge device logs and dynamic address allocations. |



Netflow collection creates compact database of observed packet streams

CONCLUSION

Network edge sensor deployments will help you get started fast and scale up early. The capabilities we've discussed here are by no means an exhaustive list, but in our experience they provide a comprehensive and manageable set of techniques for SoC operations in large organisations and even on a national level.

In this deployment model, our focus is on passive detection. Individual corporations managing their own sensors would have an option to place sensors inside their network perimeter. This will open up opportunities to augment passive detection with other techniques like active scanning, whether for vulnerabilities, network configuration changes, policy violations, or other characteristics. |



VTT TECHNICAL RESEARCH CENTRE OF FINLAND LTD will start accelerator program for drone development. Target is to boost Finnish activities to create new drone products and services as well as related business models. The program is based on a series of business case driven co-creative piloting projects created in cooperation with drone-, technology provider- and application domain end user companies. Cold climate conditions and long distances are challenges for Finnish drone operations. This fact also forms a potential foundation for building our national competitive edge in global markets, where many e.g. Utility Drone and Urban Air Mobility applications share the need for all-weather and long duty cycle operation.

Drone market globally is growing fast. Many drone-related technologies are proceeding and will make possible to create better drone products. Batteries are improving and alternative energy sources are coming to drones (eg. gasoline and hydrogen) to allow several hours operation times. Mobile cellular networks (4/5G) will replace current dedicated radio systems and will provide all-the-time connection on wide areas. More advanced sensors and cameras will be available in smaller sizes.

Regulation will allow more demanding flight operations to be done with drones. One person can operate fleet of

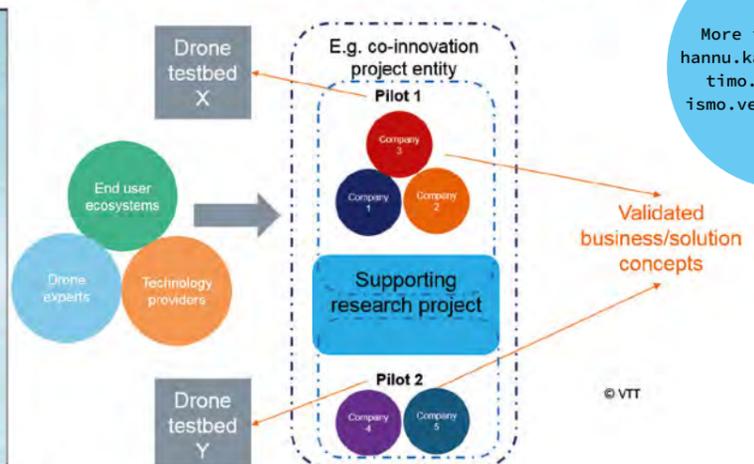
autonomous drones without visual line of sight. Drones will have increasing capability to do smart operations. UTM/ U-Space systems will integrate with ATM systems and full aviation situation map is available for all the airspace users.

Finland has lot of competencies which connects to drones. We have also special needs because of arctic climate and long distances. Low population density enables demanding technical pilots which are impossible to do in many other countries. Finnish drone regulation is liberal. Permission processes for demanding operations exist. In many areas it will be time to start drone commercial operation.

One benefit in accelerator program is to transfer learnings and information between projects. The program will gather and maintain a kind of "Cookbook of drone activities" containing analyzed best practices and lessons learned which will be shared among partners. Product and technology gaps are analyzed and new projects will be started where gaps are identified. Drones are promising platform to use for example in agriculture, forestry, security, logistics, measurements, autonomous systems. VTT invites all the interested parties to innovate together and start projects together. VTT Drone Accelerator program is part of RAAS (Research Alliance for Autonomous Systems) program. |

Drone Accelerator Finland

Target: Linking application domain opportunities with drone expertise for boosting new business. Speciality all-weather drone solutions



More information:
hannu.karvonen@vtt.fi
timo.lind@vtt.fi
ismo.vessonon@vtt.fi

“ Network edge sensor deployments will help you get started fast and scale up early. ”

WHAT IS WRONG WITH LEGACY IP SECURITY TOOLS?

text: Arimo Koivisto, XXLSEC Ltd



NUMEROUS SECURITY RESEARCHERS globally are trying to solve challenges within the legacy IP security technologies and tools. The problem is that these tools do not support future multi-connected world, but they are designed to build security between only two parties, A and B.

In the current and especially future multi-connected environments, the need for real time secure and authenticated connectivity between numerous users cannot be solved with these over 40-year-old legacy technologies like PKI and IPsec. They work nicely between two entities, A and B, but scaling the connections becomes almost impossible and creates huge management costs, vulnerabilities, risks and by carrying these old technologies as a burden it becomes impossible to meet modern scaling requirements.

It remains to be seen how security researchers see these problems regarding current encryption and authentication methods:

"The traditional methods of adding encryption and authentication to secure traffic in an IP/MPLS network typically include techniques associated with the IP security (IPsec) suite of protocols and related technologies. IPsec was originally designed to secure point-to-point Layer 3 traffic (IPsec tunnels) over an insecure medium, and did not initially target any-to-any communication for virtual private routed network (VPRN) services.

Because IPsec is designed for Layer 3 traffic, it does not adapt well to Layer 2 or other non-IP based legacy communications protocols.

*To adapt IPsec for any-to-any communication, an operator must establish a mesh of point-to-point tunnels between participating nodes. Scaling issues and the operational complexity of this solution are well known and have inhibited this approach from being adopted at a large scale to solve any-to-any communication using a point-to-point encryption approach."*¹

All future IoT networks share this same problem as default in every node which is connected to the system. Not only network elements as stated above, but also the sensors, routers, network infra, data storages, cloud services, personal devices and other end terminals in the IoT system must have authenticated and encrypted connectivity.

TOWARDS ZERO TRUST

Trust as a foundation for security is not anymore valid due to reasons, mainly geopolitical, meaning countries do not trust vendors and technologies. This means that technologies and IT-systems cannot anymore include hardware or software components which are not validated and audited. Current security environment is untrusted and trust must be defined again. Zero Trust is a requirement for the future - trust nothing and verify and authenticate everything. Security by design – not as addition.

*"Zero trust is a cybersecurity strategy that embeds security throughout the architecture for the purpose of stopping data breaches. This data-centric security model eliminates the idea of trusted or untrusted networks, devices, personas, or processes and shifts to multi-attribute based confidence levels that enable authentication and authorization policies under the concept of least privileged access. Implementing zero trust requires rethinking how we utilize existing infrastructure to implement security by design in a simpler and more efficient way while enabling unimpeded operations."*²

The question is how to do this. How can we create a solution which resolves this problem. This means that current 1990's internet security technologies like IPsec, SSL, PKI, ECDH, VPN, etc. are not the answer. New technologies are needed. Solving multi-party authentication and encrypted IP traffic is also the vision of US DoD.

*"Initial priorities included retirement of 20-30+ years old technologies, transition from point-to-point to network-centric cryptographic systems, and countermeasure actions in response to continued advances in computer processing power which enhanced adversary capabilities against DoD systems."*³

IDENTITY CONSTELLATION (IDC) – MULTI-PARTY SECURITY PROTOCOL TO REPLACE LEGACY TECHNOLOGIES

IDC is the first protocol that can deliver multi-party authentication and security, while current protocols are between two parties only. This will be the game changer. IDC can deliver shared secrets and security between numerous of nodes in a defined group.



Helsinki-East Aerodrome - where the future of aviation takes flight

text: Eija Korjula, Partner, Redstone AERO Ltd

As DoD sees, all the elements in the data transmission chain should be validated and authenticated. IoT systems, where critical data is handled, have the same requirements:

"The main purpose of identity management is to manage the life cycle of identities and provide identification, authentication and access control services for identities. There are various identities that serve different purposes in the IoT approach, but the main ones are for device and user identification. The others are used for management of devices, functions and services. Identifiers and keys are also used to sign data, including software and firmware. These different device identities are needed to identify the devices for connectivity within the access and network domains, and to identify device applications in the IoT platform and cloud domain." 4

These requirements cannot be fulfilled with PKI and IPsec legacy protocols, but IDC is capable with one user-controlled trust anchor to provide authentication and e2e encryption for all the nodes in the IoT or other IT system with minimal cost and much better security.

XXLSEC IDC is a protocol which secures cipher primitives by prioritizing dispersed secrets and usage with homomorphic encryption benefits.

LARGE SCALE IOT SYSTEMS AND 5G CONNECTIVITY
5G networks will serve especially new connected low latency high data speed systems, like vehicles, critical medical systems, drone swarms, critical communication, etc. and many times driven with artificial intelligence. Also network slicing and multicast capabilities are important features for example to critical communication users.

The question is how to do authentication and encryption with PKI and IPsec when number of sensors can be millions and millions, and they need to have same shared information available with sub1ms requirement. There is no time to do session key exchange millions of times between multiple sensors. Therefore protocols offering security only between two nodes are not good enough.

Zero Trust policy means no more trusting third-party vendors in security but authenticating all elements which handle your data, since your data is the most valuable asset the organisations have.

Secure connections have to be formed between multiple parties in real time. Same real time IoT systems require also multicast capable traffic. One node in the system will send information and many parties receive it - there is no time for millions of session key exchanges, only real time encrypted connections between multiple authenticated parties matter - and that is IDC. |

HELSINKI-EAST AERODROME, ICAO code EFPR, is a brand new professional aviation airport and test bed for integrating manned and unmanned flight. Developed and operated by Redstone Aero Ltd, the aerodrome caters to both professional general aviation and drone businesses, providing a unique European base for technological development and operational testing of unmanned aerial systems in a wide variety of scenarios, scales and flight levels. Since opening in 2019, the aerodrome has already hosted U-space demonstrations, drone Olympics and industry events and is on track to become a significant innovation center in Europe.

The greatest potential for unmanned aviation systems is commercial applications, covering a very wide range of applications and industries. Ensuring safe and predictable operation in all conditions is paramount in realizing the full potential of drones. Helsinki-East aerodrome was conceived to provide a base for multiple testing scenarios and conditions, at an optimal distance from Helsinki to provide ample free airspace and great connections. The E18 motorway runs adjacent to the aerodrome, providing opportunities to test drone logistics corridors that can also be linked with the nearby commercial ports in the city of Kotka.

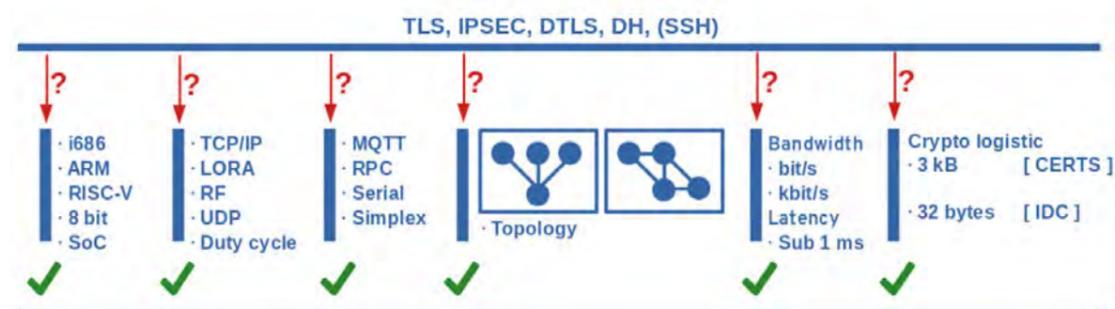
Current aerodrome infrastructure includes a 1000m paved runway, hangar space, a weather station and high altitude weather measurement capabilities. In collaboration with Business Finland and VTT, the Technical Research Center of Finland, the aerodrome will expand with a second dedicated runway for unmanned and autonomous systems and a 5G network for testing and developing new drone services. The new Drone Center building will offer space for offices, hangars, workshops and events, acting as the hub for the growing drone industry in Finland. New businesses will be created and nurtured through the Drone Accelerator program with VTT, helping start-ups and corporation develop new products and services.

The drone services market is estimated to grow to 40 billion euros in the next 5 years and is expected to generate 150 000 new jobs in Europe alone. Finland offers a fast track to developing businesses that can be scaled up throughout Europe, as Finland's flexible legislation and well-connected innovation ecosystem allow new solutions to be developed efficiently. Helsinki-East Aerodrome Drone Center is an easily accessible, comprehensive test center with a unique offering - world-class innovation networks, test infrastructure and operational environments at an operational airport where the future of manned and unmanned aviation is developed side by side. |

Public references:

- 1 Application note Network group encryption - Nokia
- 2 US DoD Digital Modernization Strategy 6/5/2019
- 3 US DoD Digital Modernization Strategy 6/5/2019
- 4 End-to-End security management for IoT, Ericsson.

Currently available authentication & security protocols can not support different combinations in modern IoT and other network connections



IDC : Next generation multi-party consensus protocol which supports all possible combinations above

- All functionalities in the same protocol -



PROTECTING WATER UTILITY AGAINST NATION STATE CYBER ADVERSARY

text: Mikko Kenttälä, CEO, SensorFu Oy



WATER SUPPLY PROFESSIONALS and government planners have long been aware that urban water systems are a lucrative target for cyber adversaries. Water utilities are heavily using industrial control system (ICS) networks to control the physical processes essential to water treatment and distribution systems. Network isolation and segmentation are key protections that prevent unauthorized access to these SCADA/ICS systems and to keep hostile adversaries at bay.

Locked Shields is a unique international cyber defence exercise offering the most complex technical live-fire challenge in the world. In 2019, a water treatment facility was part of targeted critical infrastructure. This article describes how SensorFu Beacon, a continuous network leak

detection solution, was successfully used by a defending blue team to continuously maintain isolation of water utilities SCADA/ICS network while facing skilled and motivated adversary.

LOCKED SHIELDS SCENARIO OVERVIEW

Scenario of Locked Shields 2019 exercise as described by the organizer NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE) is:

The participating Blue Teams play the role of national rapid reaction teams (RRT) that are deployed to assist a fictional country in handling a large-scale cyber incidents and all their multiple implications. In addition to maintaining around 4000 virtualized systems while experiencing more

than 2500 attacks, the teams must be effective in reporting incidents, executing strategic decisions and solving forensic, legal and media challenges. To keep up with technology developments, Locked Shields focuses on realistic scenarios and cutting-edge technologies, relevant networks and attack methods.

According to the scenario, a fictional country, Berylia, was experiencing a deteriorating security situation, where a number of hostile events coincide with coordinated cyber attacks against a major civilian internet service provider and maritime surveillance system. The attacks caused severe disruptions in the power generation and distribution, 4G communication systems, maritime surveillance, water purification plants and other critical infrastructure components. While the aim of the tech game was to maintain the operation of various systems under intense pressure, the strategic part addresses the capability to understand the impact of decisions made at the strategic and policy level.

Water utility was considered as a critical capability for Berylia. Disruptions in water distribution, including water contamination, and unavailability would provide political and strategic advantage for adversary and cause significant harm to Berylian citizens and to other nation wide operations.

To protect water treatment facility, one of the blue teams in charge of cyber-defense followed best practises in implementing and operating ICS network. In particular, this blue team focused on three parts of a control system that they wanted to secure:

1. Network communications.
2. Base operating systems of each host and ICS system.
3. Control System applications themselves.

Based on industry best practices and on-site analysis blue team utilized five methods of closing identified weaknesses or mitigating their impact:

1. Blocking or limiting access to resources and services.
2. Detecting malicious activity.
3. Mitigating impact of possible attacks.
4. Fixing core problems via e.g. operating system patches and updates.
5. Defining and implementing security policies.

Blue team based their defensive strategy on intelligence sources that they were facing cyber terrorists or nation-state adversaries with focus on the critical infrastructure of Berylia. Based on the aforementioned guidelines they implemented a layered defensive posture built around the assets in a manner that should block all but most sophisticated adversaries to gain access to assumed objectives (data munging, integrity alteration, data destruction, system destruction). Ultimately blue team based their defensive strategy on the realisation that capabilities of the attacker are not bound by their imagination nor are they infallible in building defensive measures as intended³.

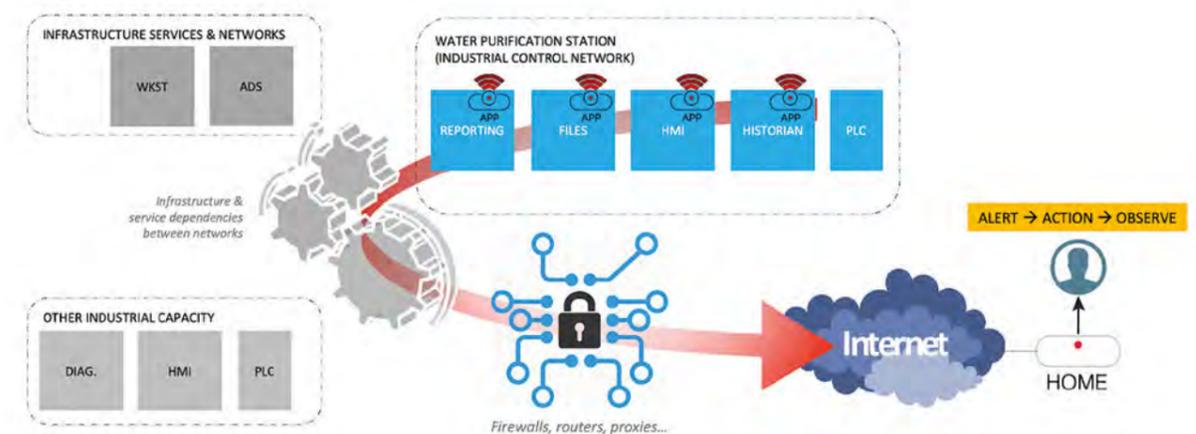
NETWORK TOPOLOGY AT THE WATER UTILITY

One of the goals of Locked Shields exercises is to evaluate cutting-edge technologies and their effectiveness in life-like cyber-war. SensorFu network leak detection solution was one of the technologies that got their trial by fire in this years exercise.

SensorFu Beacon is a software product that detects new network leak paths from isolated networks or network segments. These leak paths can be a result of human error or malice, and they may violate your security policies or contractual obligations. Product consists of two parts: Beacons that continuously look for new network leak paths by the means of active network-fu, and Home that listens for successful escapes and is used to create and manage Beacons.

Beacons were deployed to isolated portions of water utility ICS network on critical servers. These assets were crucial for securing sound water purification process. Beacons provide a capability to detect network reachability changes

Network topology and SensorFu Beacon at water utility



that may occur unintentionally or intentionally on either host based network security configurations or within larger network scope.

HOW SENSORFU BEACON SAVED THE DAY

During the course of exercise it became necessary to install patches and updates to the various hosts in water utility's office network and in the ICS environment. One of the devices updated was a firewall that controlled access to and from ICS network. During the update, the team also had to update rules on the firewall. Although updated rule set was implemented using utmost care, a mistake slipped in that allowed TCP over IPv6 to be routed to and from isolated ICS network.

Accidental and unintentional opening up of IPv6 connectivity to ICS network could have allowed reaching some of the systems not designed or intended to be exposed to unauthorized access. Furthermore it would have opened a command and control channel directly to the heart of ICS network to activate and control malware that might have been already in place.

Within minutes of deploying flawed rule set, SensorFu beacon as part of it's continuous verification cycle was able to:

- Detect a leak in the water purification segment related to network isolation, more specifically IPv6 firewall rules.
- Alert appropriate staff in defending blue team.
- Provide actionable information to the Blue-team and IT-staff to isolate the problem and take corrective action.
- Provide evidence that corrective (updated firewall ruleset) action was successful and that a leak got plugged.

Rapid reaction team (RRT) was provided with timely and actionable intel from SensorFu Beacon that allowed them to block and restrict adversary movement and mitigate command and control (C2) activities needed to carry out to execute actions in attackers objectives.

During after action debriefing SensorFu's CEO Mikko Kenttälä noted:



Let us remember that we are really talking here a bunch of seasoned professionals who work with network and IT security on a daily basis; yet simple mistakes happen all the time. This mistake could've had catastrophic consequences – in our fictitious setting. What's scary is that this could well have been for real.

Statistics from a variety of industry reports[4] indicate that time from breach to discovery is often weeks if not longer. Therefore pro-active and easy to deploy technologies that can cut the attackers kill-chain before they're able to execute should be a critical part of defensive strategy for any protected asset, but especially in those that are part of the nation's critical infrastructure.

CONCLUSIONS

For critical systems that can be fully or partially isolated, testing the isolation should be a de-facto protection strategy. As with any defensive action, its correctness needs to be continuously monitored to avoid lulling into a false sense of security. In this case, a simple configuration mistake at firewall rules opened a network path to and from part of network thought to be isolated. Active network leak detection solution, in form of SensorFu Beacon, demonstrated capability to detect network misconfiguration, and alert appropriate stakeholders, be it IT staff, network administrators, security or network operations center (SOCs, NOCs), of the misconfiguration. This leads to a timely remediation of the problem. All Of This Has Happened Before And Will Happen Again. |

If critical infrastructure protection is your responsibility, please contact us at contact@sensorfu.com for product information and to hear more about our experiences in protecting critical infrastructure and ensuring network isolation. More information about SensorFu Beacon is available at <https://www.sensorfu.com/>.

1 <https://ccdcoc.org/exercises/locked-shields/>
 2 <https://ics-cert.us-cert.gov/Recommended-Practices>
 3 Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense use case https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
 4 Verizon data breach investigation report 2019 – <https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf>

DRONES IN THE ICING TEST:

Lessons learned from Ultrahack's Drone Tournament

THE ARRIVAL OF COMMERCIAL MATURE drone-enabled services will in many cases depend on whether drone platforms can deliver the 24-7-365 promise. Are commercial drones ready to fly in cold weather? Or even in icing conditions?

Ultrahack with the support VTT Technical Research Centre of Finland Ltd tested several commercial drones in the VTT Icing Wind Tunnel as part of the first ever Drone Tournament in September 2019.

The participants welcomed the opportunity to test the performance of their drone systems in the controlled repeatable conditions of the VTT icing wind tunnel facility, and provided valuable feedback regarding the test setup from a customer perspective. In the VTT icing wind tunnel, it is possible to generate temperatures between -25 and +30 Celsius and wind speeds up to 20 m/s continuously. In addition, wind speeds between 20 – 50 m/s can be achieved for short periods of time. The icing wind tunnel can be

operated in typical or severe icing conditions and droplet size level can be tuned according to different requirements.

It was seen in the tests that all the drones experienced heavy icing in the propellers after barely two minutes of exposure to harsh in-cloud icing conditions (with -5 Celcius and a wind speed of 10 m/s). The test setup involved measurement of the lift generated by the drones, which soon dropped to below 80% of the reference lift for horizontal flight.

One of the drone was tested in free flight in front of the icing tunnel, and was able to sustain horizontal flight for several minutes even with significant ice accretion. However, this was at the cost of an increased power consumption.

VTT is currently looking for partners interested in studying and testing drones and drone components with different kind of solutions (e.g., coatings) to prevent drone icing in cold conditions. |



Icing starting to form in the blade of the drone in VTT's icing wind tunnel.



VTT experts installing one drone in the icing wind tunnel for test purposes. No drones were harmed in the making of these tests.

Contact information:
 VTT TECHNICAL RESEARCH CENTRE OF FINLAND LTD
 Tuomas Jokela Raul Prieto
 tuomas.jokela@vtt.fi raul.prieto@vtt.fi
 +358 40 8466497 +358 40 1439018

Disinformation threatens democratic processes, BUT POTENTIALLY ALSO YOUR BUSINESS

text: Pasi Eronen

Foreign powers and fringe elements want to undermine the democratic processes and faith that the citizenry has in them with disinformation operations in order to reach their goals and support their political agenda, but disinformation may also threaten your business.

FOREIGN POWERS and various societal fringe elements, such as populist movements, conduct disinformation campaigns that support political and ideological extremes, sow confusion and division, and exploit the existing societal vulnerabilities. In short, they are lending their helping hand to allow societies to tear themselves apart.

The disinformation operations have been reported to use variety of tools, such as remotely organized agenda-driven gatherings, paid advertisement, government controlled or political agenda driven news outlets, online bots and trolls, paid-for local operators, and various kind of front organizations, such as research centers and think tanks, to push out biased reporting, blatant lies, and leaks to the targeted audiences in order to influence their opinions and actions.

As intelligence reports from the U.S. and from European countries have confirmed, foreign influence efforts operate in an integrated and networked manner. Disinformation operations are supported with information obtained from espionage operations.

Such operations have included in addition to remotely conducted parts using cyber means, also teams that have been deployed in the field to have an access to hard to reach targets. Targets have not been limited to the members of government, political parties and their representatives, and other political operators, but the foreign operators have cast their information collection network wide to include news reporters, think tanks and their subject matter experts,

defence contractors, and civil society organizations and activists.

Waging an active disinformation campaign supported by cyber operations demand vast preparations. In addition to the typical preparations, such as conducting reconnaissance to understand the target, building the tools to penetrate and stay in systems, and having supporting technological infrastructure; it is also necessary to have other operations supporting elements in place, such as fake identities in target countries, ability to store and transfer financial resources. Moreover, as collected information needs to be released into public realm for the wanted effect, a network of self-created proxies and like-minded external parties is needed together with means of amplification such traditional media outlets with local and global reach.

Knowing the adversary and their vulnerabilities is in the key role for efficient disinformation operations. By taking advantage of already existing political ambitions, identified inflammatory political issues, grievances felt by minorities, and viral and rapidly growing popular movements, the influence operations by foreign powers and fringe elements can gain leverage and momentum that would be harder, or even impossible to achieve artificially. Thus, some of the work in disinformation operations is conducted knowingly or unwittingly by local opportunists, political operators, and unsuspecting idealists. Moreover, the perpetrators work seems to be in part supported by the social media platform providers through their engagement feeding and advertisement targeting algorithms and platform monetization models.

In addition to the short term impact, continued barrage of disinformation helps to shape the information sphere in a longer term, and make audiences more receptive to messaging or concrete actions following later. Change of narratives, accepted truths, and preferences over ideologies and topics may happen relatively slowly, in small

increments, not necessarily in a revolutionary manner. Some lies and manipulations that have been successfully inserted to the shared knowledge base may continue to bear fruit for decades to come and change the strategic environment gradually towards the preferred one.

It appears that influence operations that are utilizing disinformation and supporting cyber elements offer a good return on investment. Public sources have estimated that the disinformation operation linked to the U.S. presidential elections back in 2016 spent a few millions of dollars during more than two years of operations. Similarly, a nation state linked cyber operation that stole vast troves of sensitive airplane design information from the U.S. was estimated to have spent around a million dollars during its activities. In contrast to these figures, one strike volley of cruise missiles can be estimated to cost tens of millions of dollars.

Thus, it is no wonder that the foreign powers seem to have found the results of their influence operations worth the investment in money, time, and personnel, as they have continued to apply the same playbook in referendums and elections across the Europe both prior the U.S. elections and after them.

Spread of disinformation has in recent years been mostly covered in the context of nation states and fringe factions meddling with our democratic processes, but disinformation is also a potent vehicle to influence companies and their employees, and even disrupt the markets that they operate in.

”
Disinformation is also a potent vehicle to influence companies and their employees, and even disrupt the markets that they operate in.

It is not far fetched to think that similar tactics could be used against commercial targets having links to an ongoing conflict, or some other strategic interests. Known linkages and exposed activities could be weaponized in publications targeting the selected audiences using social media, alternative media platforms, and even traditional media. Weaponized information could be primed to frame companies' activities in unwanted context, or to appear to be unethical, or against the norms and goals of the target audiences. In addition to companies, also singled out employees could be utilized for this purpose and as targets of intimidation.

If the risk benefit calculation is rewarding enough, companies, their operators, and clientele could be targeted with an integrated influence operation combining cyber and information elements, where company's information systems would be penetrated, information would be gleaned from them, and the information would be leaked to public in order to hamper, or even stop the ongoing business operations, such as offering support for military in their operations or in research and development, and to spoil and poison the existing client relationships with authentic or manipulated content, such as shallow and deep fakes.

Therefore, it is worthwhile for the companies to understand how influence and disinformation operations work and what are some of the tactics and tools used. Moreover, it is important to map out as a part of threats and risks identification process how company may end up being tangled in such operations either as a target, or as a collateral damage, and how that risk can be mitigated and what are the potential response mechanisms should that risk realize. |

Cybersecurity in smart cities

This report aims at generating awareness of the challenge of cybersecurity that lies ahead of us and the means of overcoming it.

IOT PROVIDES SIGNIFICANT ADVANTAGES, but it comes along with associated cyber risks. As the government gets more and more familiar with the benefits that IoT can deliver – specifically for smart cities – key concerns around security, privacy and trust are likely to grow. A comprehensive understanding about the cybersecurity threats that these technology brings is being still worked upon, but its rapid adoption is exposing potential security breaches.

Security and the IoT ecosystem



WHEN IT COMES TO THE INTERNET OF THINGS (IoT), you can believe the hype. IoT will likely be bigger than most people think and it presents great opportunities for innovative Australian businesses to lead the way.

But success in the IoT space will take more than slick applications, connected devices and advanced analytics; it will also require a robust approach to security, privacy and trust.

For the technology sector, the message from businesses and consumers is clear: be innovative, be bold and be secure. IoT will bring massive growth to tech companies and IoT developers that can carve out a dominant position in this expanding market.

However, with evolving market maturity and heightened competition has come mounting concern for current and

potential IoT users, particularly around security.

This report suggests tech firms and IoT service providers will need to work quickly, diligently and decisively to deal with concerns related to security (how well controlled is the device and the infrastructure?), privacy (how is data kept confidential?) and trust (how is customer confidence being addressed?), before they turn into problems. Those that fail to do so will have a difficult time growing in this new environment.

The technology sector must come together with other vertical and horizontal players in the ecosystem to create a unified approach to security and standards that everyone can live by, and grow with. Today's current state of fragmentation and competition on standards will only result in greater complexity for users and reduced growth for the IoT sector.



Scan the QR to read full article

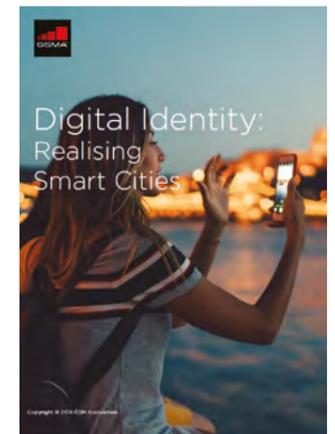
Digital Identity: Realising Smart Cities

Scan the QR to read full article



SMART CITIES will prove the Internet of Things' most visible manifestation. We can already see urban environments becoming increasingly connected, as the practical elements of city life start to come online. The arrival of smart parking, for instance – the ability to seek and allocate parking spaces in advance, keeping unnecessary driving time to a minimum – has brought with it a range of improvements to congestion, pollution, driver convenience and city revenues. Municipal authorities can now also enhance the safety and economic performance of their cities through smart traffic systems, using the data their roads

generate to manage vehicle flows in real time. And smart utilities are now poised to become a phenomenal growth area in bringing smart cities to life: the majority of European energy customers and vendors alike are set to enjoy the benefits of remote metering by 2020, which will reduce costs, inaccuracies and time lost for all concerned. As we look further ahead to the mid-century, however, intelligent public services will move beyond the mechanical: two decades from now, increasingly complex and sensitive aspects of our lives will be connected to city infrastructure via IoT.



Connected Cities

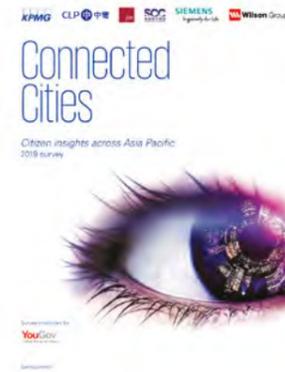
Citizen insights across Asia Pacific

OUR CONNECTED CITIES: CITIZEN INSIGHTS ACROSS ASIA PACIFIC report tracks the current state of smart city development in five Asia Pacific urban centres: Hong Kong, Melbourne, Seoul, Shanghai, and Singapore.

The survey seeks 4,192 residents' opinions on the smart city development areas that are most important to them as well, as what benefits they expect as their cities become 'smarter'. It takes a detailed look at progress and key development actions needed in six key areas: transportation and mobility, building a future-focused workforce, living environment, healthcare, energy and resources and technology solutions.

This year's study builds on our inaugural Connecting Hong Kong report published in January 2018. In that study, we defined what makes a 'liveable city'. In addition, for a city to be smart, its government needs to be conscious of the needs and wishes of its population and the potential impact – both positive and negative – of technological developments. This includes measures to enhance liveability by creating public amenities and promoting overall quality of life.

To further complement these findings, we include viewpoints from senior private sector and NGO practitioners, as well as case studies that showcase best practices across the region. We hope you find the report informative and we would like to thank all the participants and contributors for their valuable insights. |



Scan the QR to read full article



”
In addition, for a city to be smart, its government needs to be conscious of the needs and wishes of its population and the potential impact – both positive and negative – of technological developments.

Scan the QR to read full article

Mobility 2030: Transforming the mobility landscape

How consumers and businesses can seize the benefits of the mobility revolution

MOBILITY IS UNDERGOING one of the most transformational social, technological and economic shifts of a generation, shaped by three key disruptive forces: electric vehicles and alternative powertrains, connected and autonomous vehicles and on-demand

mobility services. Sectors are being disrupted, with new markets emerging, while others are converging, and some are disappearing entirely. The winners are likely to be those that can truly understand the impact and timing of disruption, and seize the right emerging opportunities. This means swiftly adapting business and operating models and securing the right partnerships and acquisition targets. |

How autonomous vehicles and intelligent transport networks create a smart city

Our podcast explores how cities of the future look – where you go anywhere, anytime, without any need to work out a route, look up a timetable, buy a ticket or pay a fare.

INTELLIGENT TRANSPORT will fundamentally change the way cities operate – and it's only a few years away. This is not just a transport revolution, but a societal one.

Listen to our podcast as Partner and Head of Infrastructure Building & Construction, Richard Threlfall explores how intelligent transport networks and autonomous vehicles create not only stress free commutes, but also quieter and greener cities. |

Scan the QR to listen the podcast



SMART INFRASTRUCTURE: INTELLIGENT TRANSPORT

Listen to our podcast about intelligent transport networks and autonomous vehicles.



SIMPLIFYING IOT CONNECTIVITY

When it comes to IoT,
simplicity is security

As the IoT trend continues to grow, there isn't a single area of our life that won't be touched by IoT devices in the next decade. Connectivity is the foundation for IoT, and it needs to be simple and secure for companies to be able to reap the benefits.

THE NEED FOR RELIABLE INTERNET connections is greater than ever, with estimates of billions of devices being connected already today. IoT is expected to explode the number of connected objects to 25 billion by the year 2021, producing immense volumes of data (Gartner). The global IoT market is said to expand to \$457 billion by 2020 (IDC). Thus, also the demand for ubiquitous connectivity is bound to continue to grow at an unforeseen pace in the coming years.

IoT consists of intelligent, connected machines and devices that gather and use vast amounts of data to accomplish things that we could not even dream of a few years back. Expectations are high regarding market opportunities and new business models, especially regarding the so-called Industrial Internet of Things (IIoT).

POTENTIAL FOR SAVING AND CREATING NEW

What makes IoT interesting for companies are the various use cases and their significant potential. Devices such as elevators, factory equipment and work spaces are being connected to the internet to transmit data from their background processes. Real-time data collection and data logging help companies extract the data for analysis, in the hopes of boosting efficiency. One popular use case for IoT is predictive maintenance, which means analyzing historical data to predict when maintenance is needed.

By harnessing data companies can use remote access to improve their operating efficiency and uptime as well as productivity. A better service performance will also improve customer satisfaction. In addition to the remarkable saving potential in remote services, IoT brings along business oppor-

tunities from new services or operations that the companies previously did not provide, and generate new lines of revenue.

SIMPLIFYING IOT

To do all this, a feedback to devices is needed. Companies need IoT connectivity for data collection and remote access. But before the IoT can really live up to the promises, challenges with cyber security, lack of standardization and skilled workers, legacy-installed base, significant upfront investments and data integrity must be solved (Morganstanley.com). Basically, any "thing" connected to and controlled by Internet-connected networks is vulnerable to being hacked.

IoT projects typically require exchanging OT (operational technology) data with IT systems, and this collaboration between OT and IT stakeholders is already in process. However, the impasse often occurs around the topic of cyber security. Enterprise IT departments understand the need for security, but often discount operation's need for ease of use and efficiency. Conversely, operational teams (who also understand the reasons for cyber security) underestimate the complexity of securing data transfer, access control, in these multi-tiered network environments.

As secure connectivity becomes essential, we have taken connectivity and made it simple yet highly secure. By eliminating human errors and other cyber security threats in IoT connections, companies will be able to feel confident and enjoy the benefits of IoT. When we connect ourselves to the web, trust is the best currency. To be able to trust that security risks are acknowledged and prepared for, would mean endless business opportunities. What would you do?

Security, reliability and simplicity are exactly what Tosibox offers. They are what makes us a globally sought-after provider of secure digital connectivity. The game changing TOSIBOX® technology is used in more than 120 countries. |

Jarno Linnéll
CEO, Tosibox
Professor of cybersecurity, Aalto University



2-3 October 2019
Messukeskus Helsinki

THE MOST SIGNIFICANT EVENT
OF CYBER SECURITY SOLUTIONS
IN NORTHERN EUROPE

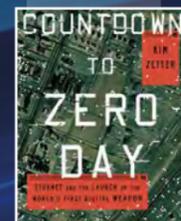
SEMINAR TOPICS 2019

Politics of Cyber Security – Cyber affects our world in visible, invisible and hidden ways. Who sets the rules and who obeys them?

Reality of Cyber Security – Cyber is like globalization – even if you think you are not part of it, you are. What does this mean to you?

Future of Cyber Security – AI, IoT and Machine learning are all dependent on cyber security. How come, and what comes next?

Economics of Cyber Security – Cyber is a key requirement for established trades and an enabler of new businesses and a. Those who master the connection will lead the way.



Kim Zetter,
Award-winning
investigative
journalist and author



Tom Van de Wiele
Principal
Cyber Security
Consultant



Rik Ferguson
Vice President
Security Research



Mark Galeotti
World's leading specialist
on Russian crime and
security issues

Tickets and programme: cybersecuritynordic.com

Organizers:



Strategic Partners:



ORBITER 4
Small Tactical UAS



Ahead of Time

PEGASUS 120
Tactical VTOL UAS



ORBITER 3
Small Tactical UAS



DOMINATOR XP
Medium Altitude Long Endurance UAS

