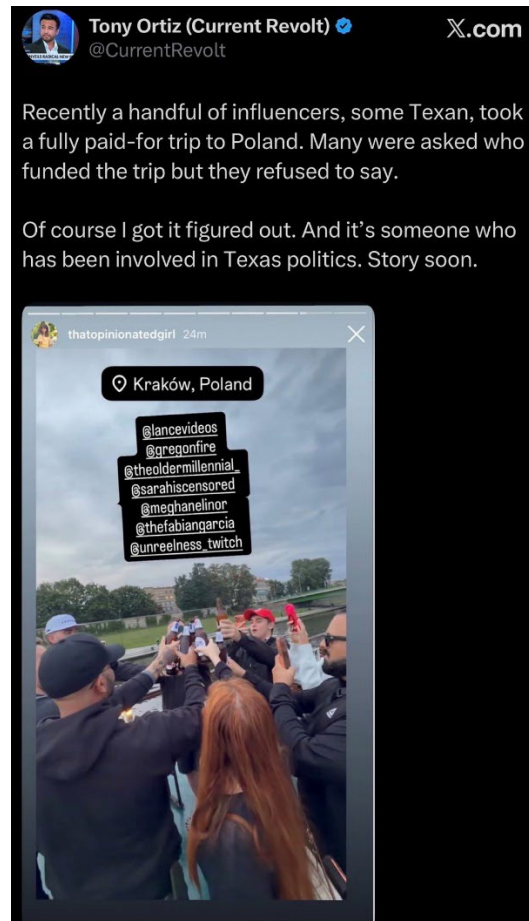


Why did certain influencers going to Poland have interactions with something possibly natsec related with our cognitive warfare?



What is the esa?

1. European Security Academy (ESA)

[European Security Academy](#) (often abbreviated as **EUSECA** or **ESA**). Based primarily in Poland, this is a world-renowned private military, law enforcement, and private security training contractor. [1, 2]

They operate a massive 120-hectare [Special Forces Training Center](#) that hosts active special units from around the globe. For civilians, veterans, and contractors, they offer intensive, high-risk tactical courses. [1, 2, 3]

- **EUSECA PMC Course:** A 7-day course tailored for operating in hostile regions like the Middle East or Central America. It covers small group tactics, reconnaissance, convoy security, and live-fire drills. [1]
- **EUSECA CPO Course:** A comprehensive 14-day training program combining VIP protection theory, security driving, and realistic urban force-on-force scenarios. [1]
- **EUSECA Military Boot Camp:** A high-intensity, military-style course designed by special operations veterans to test physical limits, teamwork, and mental resilience under pressure. [1]

2. European Space Agency (ESA)

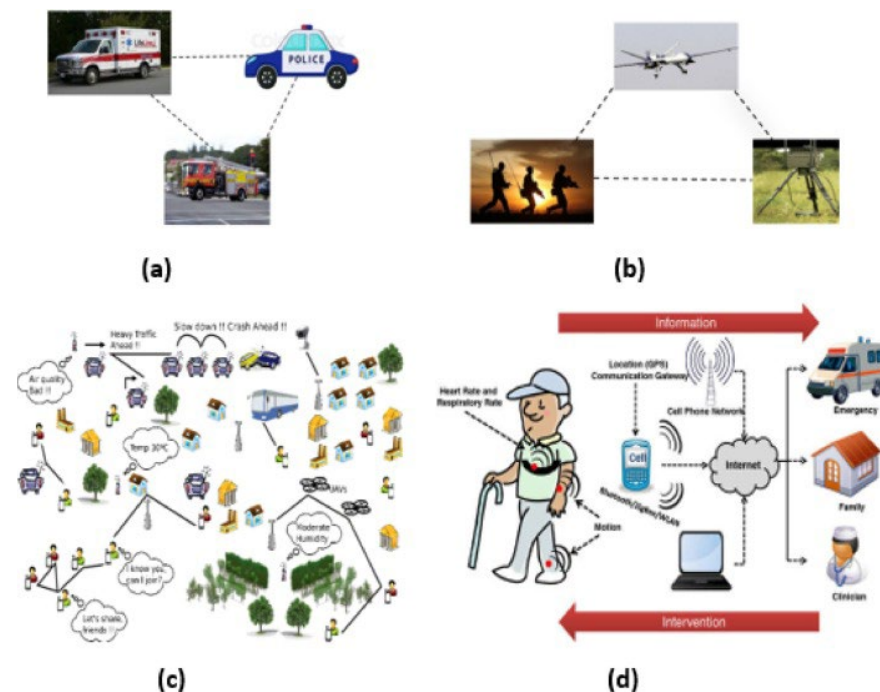
their astronaut candidates undergo grueling **survival training** that heavily mimics military SERE (Survival, Evasion, Resistance, and Escape) schools. [1, 2, 3, 4]

Coordinated at the [European Astronaut Centre](#) in Cologne, Germany, this training prepares astronauts for the possibility of an emergency landing in extreme, remote environments. [1, 2]

- **Extreme Environment Survival:** Astronauts are dropped into wilderness areas (such as the Pyrenees or open sea) where they must build shelters out of spacecraft parts, scavenge for food, and handle extreme cold or heat. [1, 2]
- **Water & Sea Survival:** Co-hosted with European coast guards, candidates practice escaping capsules in rough open water, righting life rafts, and surviving maritime conditions. [1, 2]
- **Psychological & Stress Prep:** This training is explicitly designed by the Astronaut Training Team to build cohesion, fast decision-making, and psychological endurance under severe physical stress. [1]

<https://www.euseca.com/>

- **For the European Space Agency (ESA):** If a U.S. company performs classified contract work involving international/European space agencies for NATO, they must navigate the **Facility Security Clearance (FSC)** and **Personnel Security Clearance (PSC)** frameworks rather than standard DODIN impact levels. [1]

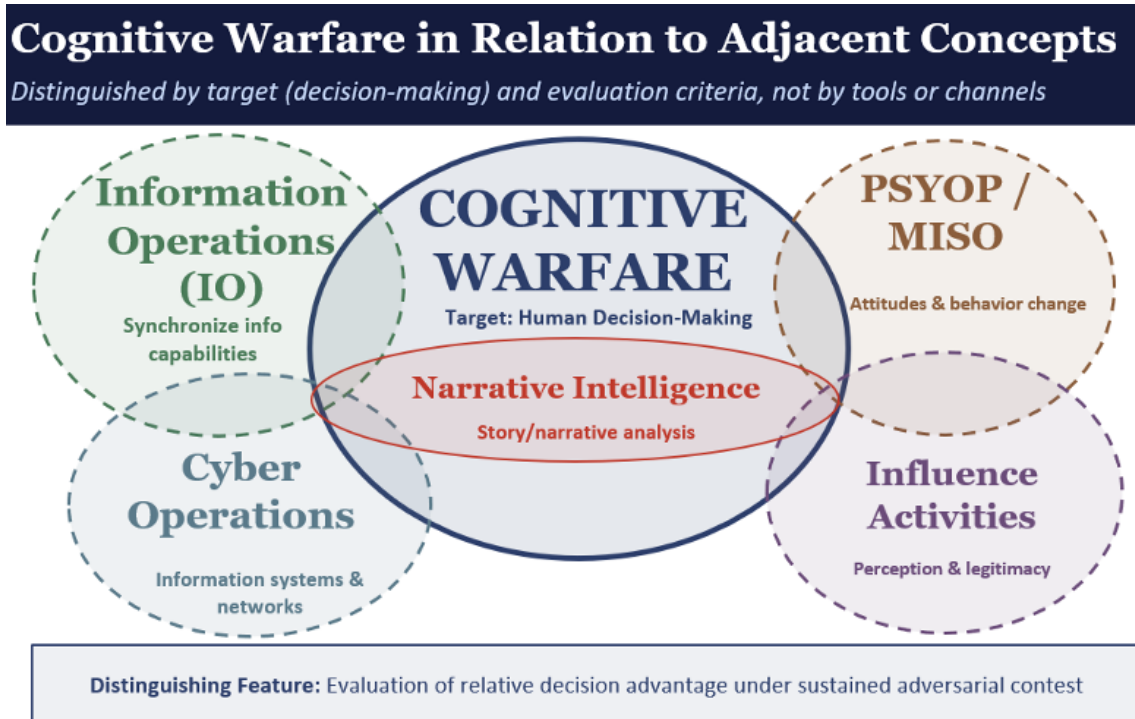
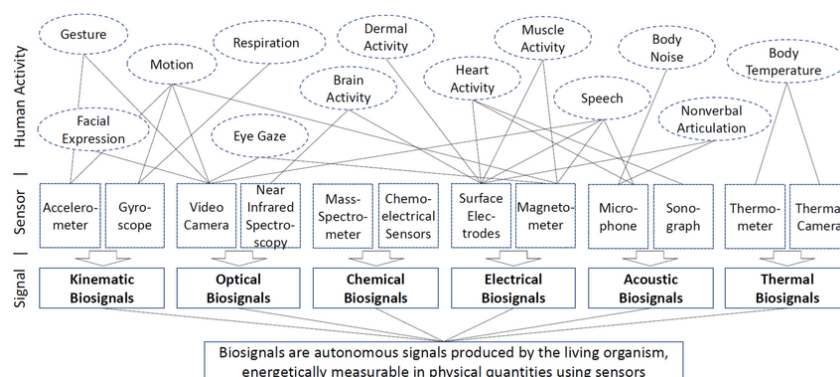


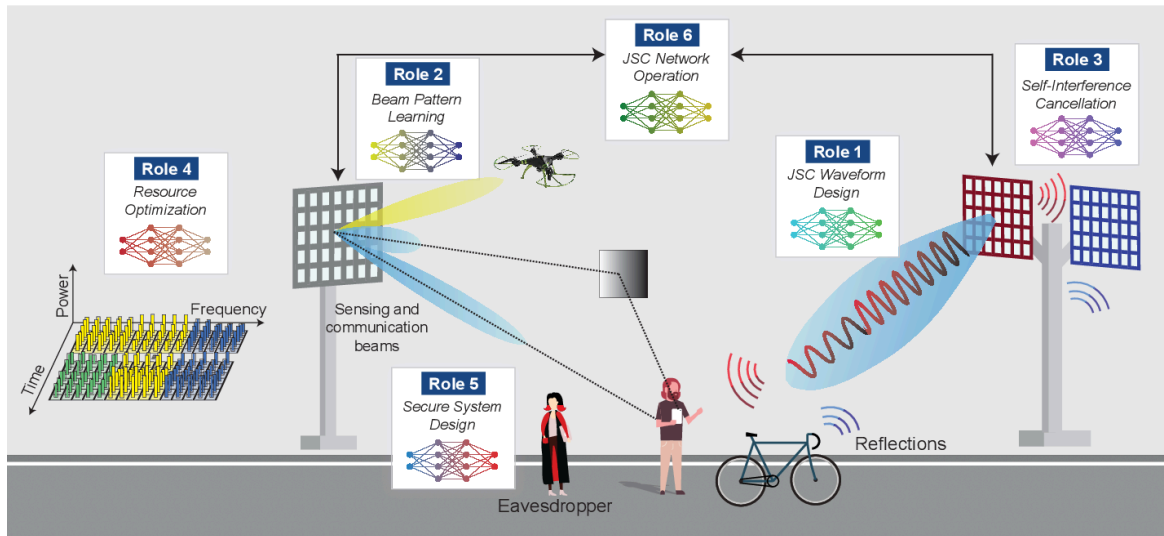
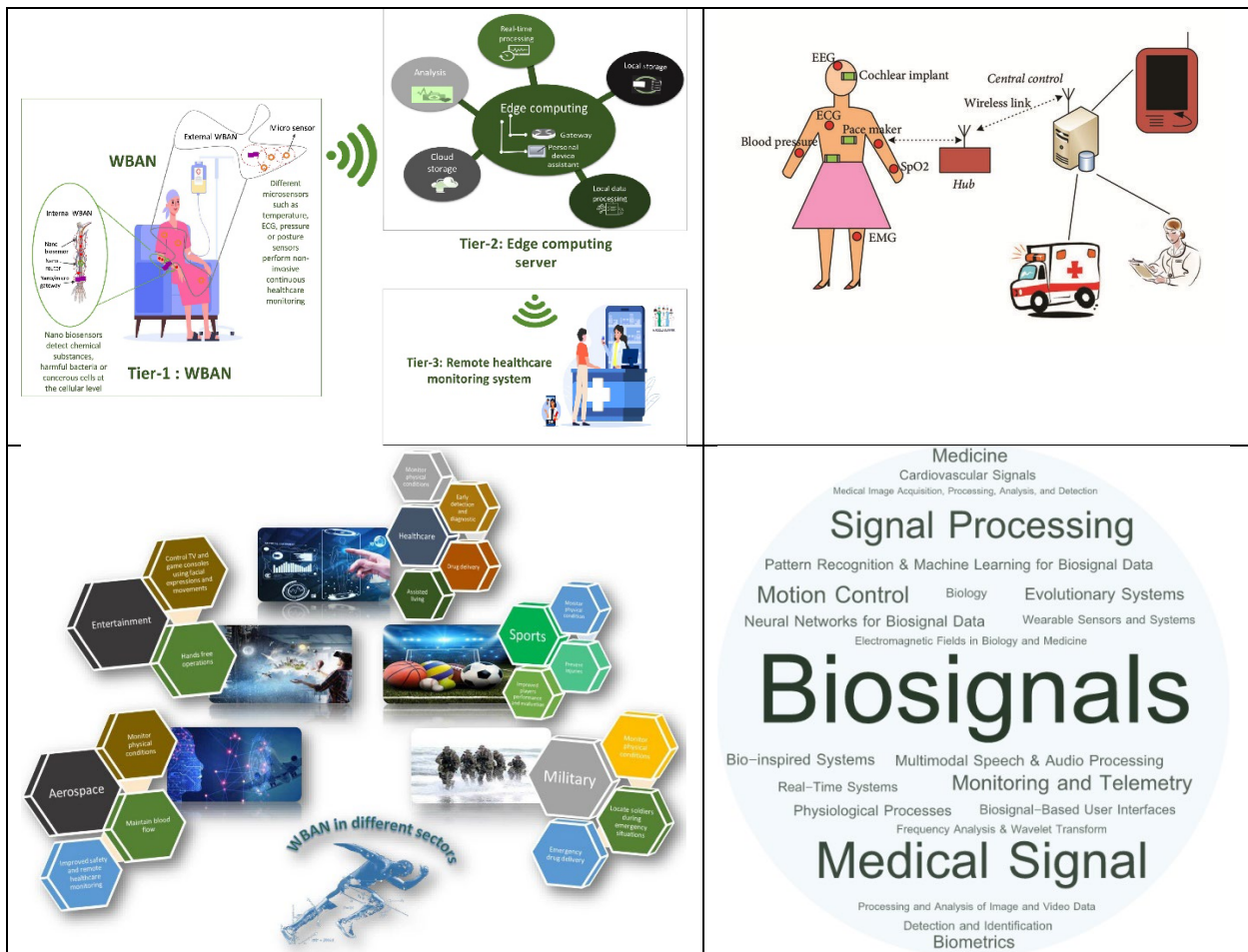
The United States does not have a single direct corporate equivalent to the [European Security Academy](#) (ESA), but elite private tactical, firearms, and high-risk executive protection training is provided by prominent private U.S. entities like **Sig Sauer Academy**, **Gunsite Academy**, and **Blackwater/Academi** legacy training providers. [1, 2]

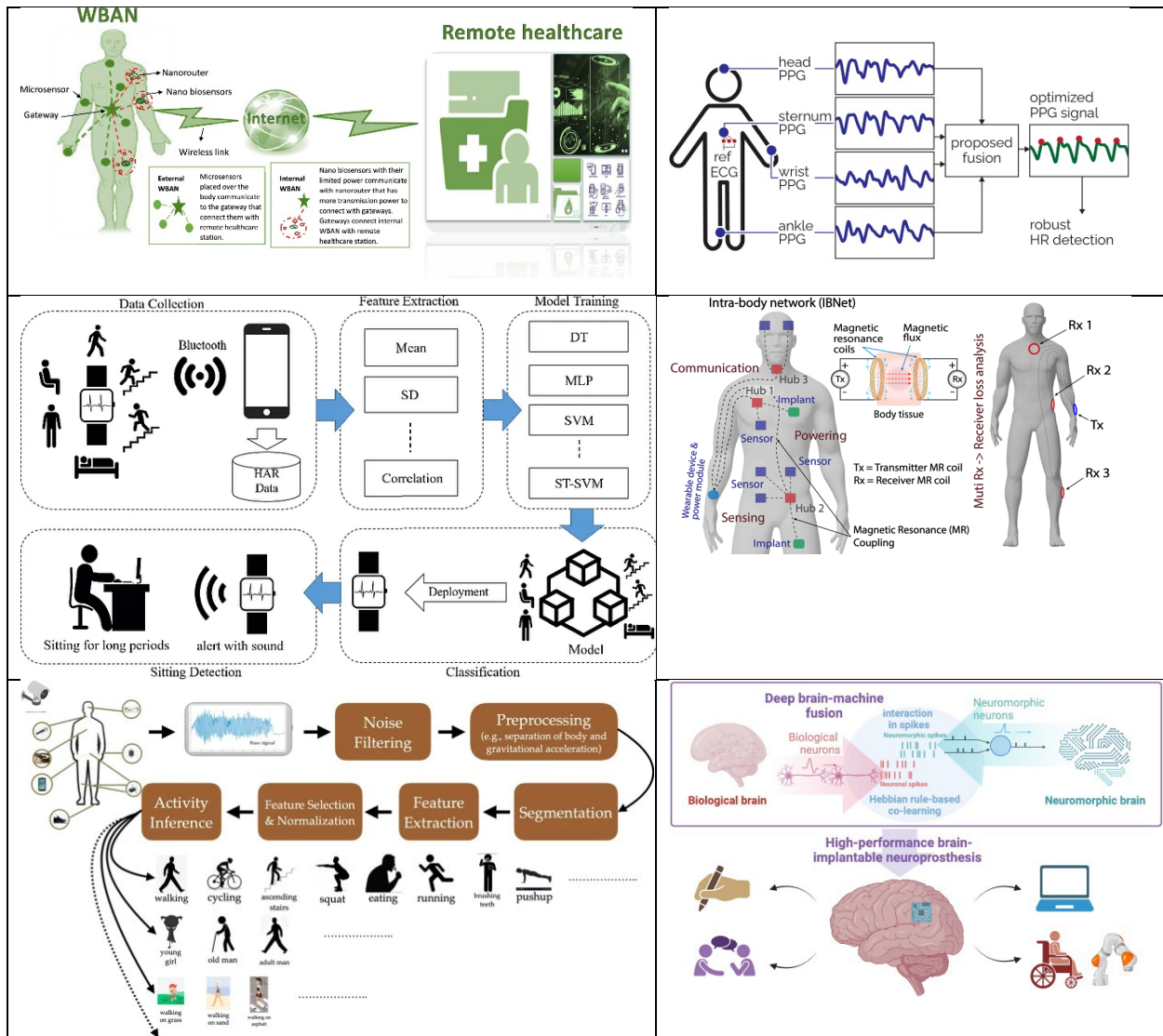
Top U.S. Equivalents by Specialty

- **High-Risk and Private Military Contractor (PMC) Training:** Companies like **Academi** (formerly Xe Services / Blackwater) and various specialized overseas contracting training providers offer hostile environment and security detail training similar to ESA's PMC modules. [1, 2]
- **Advanced Firearms and Tactical Defense: Gunsite Academy** (Arizona) and the **Sig Sauer Academy** (New Hampshire) serve as premier private facilities for intensive tactical pistol, carbine, and defensive driving instruction for law enforcement, military, and vetted civilians.
- **Executive Protection and Bodyguard Certification:** Schools like **EPI (Executive Protection Institute)** and **Pacific West Academy** offer high-level Close Protection Operative (CPO) courses mapped to domestic and international security standards.

Sara mentioned satellites – **geospatial** – **COGNITIVE WARFARE**





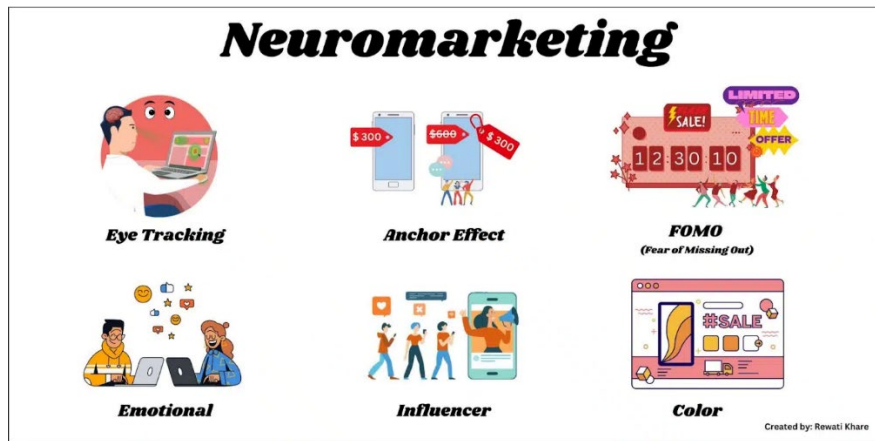
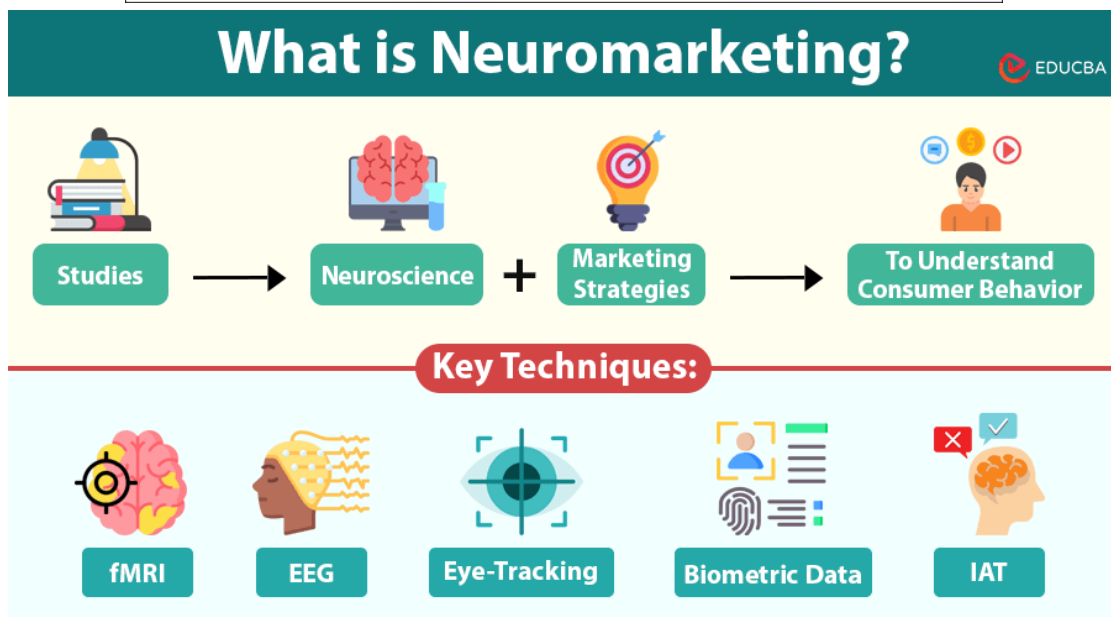


Sara mentioned yomama hearing neuromarketing (**Neuromarketing**)





<https://professional.dce.harvard.edu/blog/marketing/neuromarketing-predicting-consumer-behavior-to-drive-purchasing-decisions/>



Cognitive warfare treats the human brain as a battlespace by targeting how people think, process information, and make decisions *rather than just what opinions they hold*

- **Targeting the Mind:** The primary goal is disrupting judgment, slowing reaction times, and eroding trust in public institutions rather than seizing physical territory. [1, 2]
- **Beyond Disinformation:** While it uses propaganda and fake news, cognitive warfare relies heavily on information overload and cognitive fatigue to degrade critical thinking. [1]
- **Adaptive and Interactive:** It functions as an ongoing contest between attackers and defenders who constantly shift narratives and defenses. [1]
- **Decision-Centric:** Success is measured by how badly an opponent's decision-making loop breaks down under pressure, rather than how many people view a message

<https://www.whitehouse.gov/presidential-actions/2026/08/expanding-capabilities-to-combat-transnational-cyber-enabled-crime/>

<https://www.sto.nato.int/document/mitigating-and-responding-to-cognitive-warfare-2/>

<https://inss.ndu.edu/Research-and-Commentary/View-Publications/Article/4371195/cognitive-warfare-2026-natos-chief-scientist-report-as-sentinel-call-for-operat/>

Cognitive Warfare 2026: NATO's Chief Scientist Report as Sentinel Call for Operational Readiness

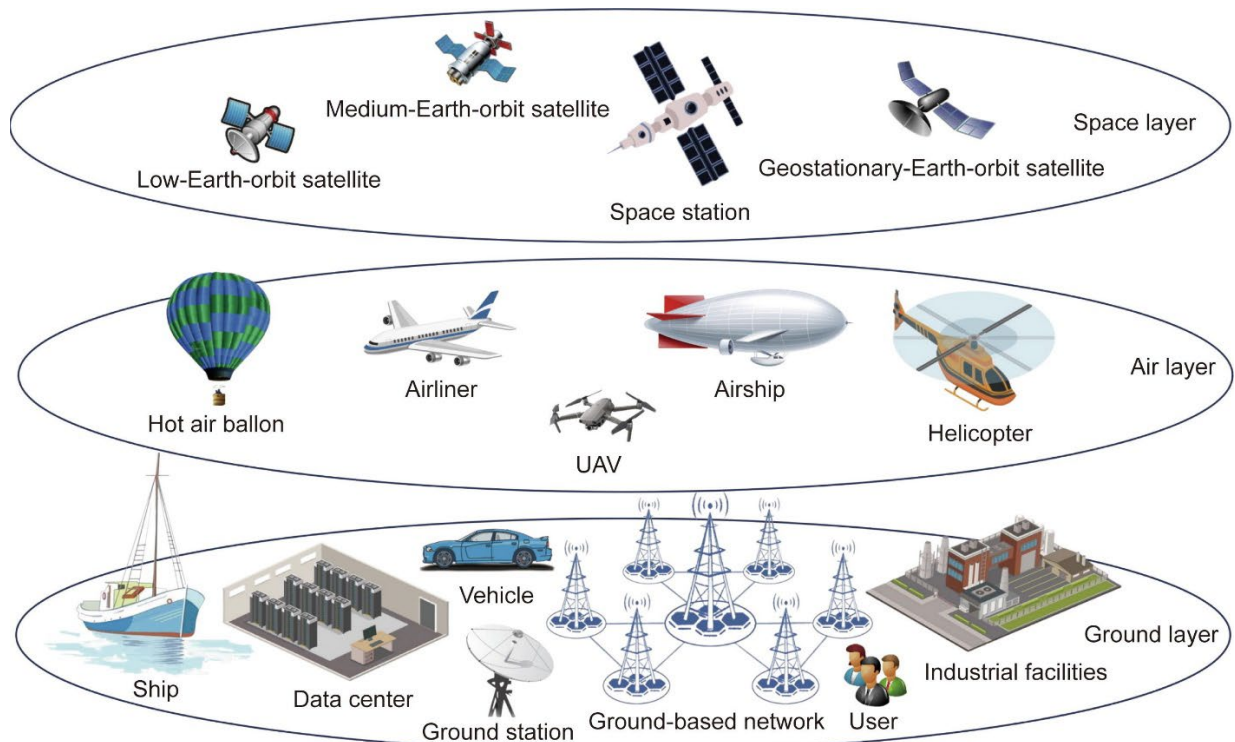
By Dr. James Girodano Strategic Insights

The recently released [NATO Chief Scientist's 2025 Report on Cognitive Warfare](#) provides a timely acknowledgment of a strategic reality that contemporary conflict is increasingly behavior-centric, and the decisive terrain is often not geographic but how individuals and groups perceive, interpret, decide, and act. I have had the privilege, honor and pleasure of working on [NATO's initial cognitive warfare studies](#) beginning in 2018, which explicitly emphasized that cognitive warfare is not merely "PSYOPS with better tools."

<https://tdhj.org/blog/post/cognitive-psychological-warfare/>

A Systematic Review Of Cognitive And Psychological Warfare

Abstract: The human mind is the paramount battleground in modern warfare, where cognitive warfare emerges as an unparalleled domain demanding recognition. The People's Republic of China and Russia have incorporated cognitive warfare and related strategies into their operations. However, there remains a blurriness regarding the concept and application of cognitive warfare in academic discourse and Western military doctrines.





INTERAGENCY
SECURITY
COMMITTEE



PROTECTING AGAINST THE THREAT OF UNMANNED AIRCRAFT SYSTEMS (UAS)

An Interagency Security Committee Best Practice

November 2020 Edition

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
Interagency Security Committee

Personnel working with Manned-Unmanned Teaming (MUM-T) systems typically require a minimum of a Secret security clearance. Because MUM-T involves advanced autonomous technologies, secure data links, and cross-domain military intelligence, security clearance requirements apply to both the active operators and the defense contractors developing the technology. [\[1, 2, 3\]](#)

The security clearance framework for unmanned teaming is structured around the role of the individual and the level of system integration.

Clearance Levels by Role

- **System Operators and Pilots:** Active-duty operators managing autonomous platforms—such as Collaborative Combat Aircraft (CCAs) or Unmanned Surface Vessels (USVs)—require a **Secret clearance** at minimum. This is due to their access to tactical data links, encrypted communications, and real-time theater surveillance. [\[1, 2, 3, 4\]](#)
- **Aerospace & Software Engineers:** Defense contractors writing autonomy software (like AI-driven flight algorithms) or designing stealth hardware must hold a **Secret or Top Secret clearance** depending on the specific program. Specialized software development often requires program-specific "read-ons" under a **Special Access Program (SAP)** to protect proprietary military capabilities from foreign intelligence. [\[1, 2, 3\]](#)

Interoperability and Information Sharing

The security clearance scope is heavily influenced by the **Level of Interoperability (LOI)** defined by NATO standard STANAG 4586: [1, 2]

- **Low Interoperability (LOI 1-2):** Involves simply receiving data or telemetry from an unmanned system. This data may sometimes fall under **Controlled Unclassified Information (CUI)** or basic Secret parameters. [1, 2, 3]
- **High Interoperability (LOI 3-5):** Involves full control over the drone's payload, flight path, or launch and recovery. Systems operating at this tier require robust cryptographic clearances and highly restricted operational networks. [1, 2]

Corporate/Contractor Requirements

For private companies bidding on MUM-T defense contracts, the requirements are two-fold:

1. **Facility Security Clearance (FCL):** The company itself must be sponsored by a government agency (like NAVAIR or the Air Force) to obtain an FCL to legally house and process classified data. [1, 2]
2. **Personnel Security Clearance (PCL):** Individual engineers and executives must successfully submit an SF-86 background investigation to receive their individual clearances before beginning work on classified components. [1, 2, 3]

https://www.navysbir.com/n22_1/N221-017.htm

221-017 TITLE: Manned-Unmanned Teaming Survival in an Adaptive World

OUSD (R&E) MODERNIZATION PRIORITY: Artificial Intelligence (AI)/Machine Learning (ML);Autonomy;General Warfighting Requirements (GWR)

TECHNOLOGY AREA(S): Battlespace Environments;Electronics;Information Systems

OBJECTIVE: Develop and demonstrate an innovative, mission effective Unmanned Air Vehicle (UAV) capability to assist manned-unmanned teaming (MUM-T) to challenge and/or negate radars and radar networks by enabling UAVs to automatically sense and communicate weaknesses in a radar and/or radar networks.

DESCRIPTION: Current airborne electronic warfare (EW) systems must first identify a threat radar to determine the appropriate preprogrammed electronic countermeasure (ECM) technique. This approach loses effectiveness as radars evolve from fixed analog systems to programmable digital variants with unknown behaviors and agile waveforms. Future radars will likely present an even greater challenge as they will be capable of sensing the environment and adapting transmissions and signal processing to maximize performance and mitigate interference effects.

<https://publicintelligence.net/cisa-unmanned-aircraft-systems-threats/>

<https://sam.gov/opp/dbc64cacc0e9402c9799c5c910bc45b4/view>

NATO Business Opportunity: Alliance Future Surveillance and Control (AFSC) Engineering Support

The NATO Support and Procurement Agency (NSPA) intends to implement International Competitive Bidding (ICB) for the provision of Contracted Engineering Support (CES) for the project entitled "Alliance Future Surveillance and Control (AFSC) Development Stage Phase 1."

To qualify to bid on this project, a U.S. prime contractor must

- 1) *maintain a professionally active facility (office, factory, etc.) in the United States*
- 2) *hold a DOD Facility Security Clearance at the level of SECRET or higher*
- 3) *be pre-approved for participation in NATO International Competitive Bidding (ICB)*
- 4) *be issued a Declaration of Eligibility (DOE) by the U.S. Government*
- 5) *be registered in the NSPA Source File:*

<https://portal.nspa.nato.int/Registration/OnlineRegistration.aspx?lng=en>

In most cases, the consultants will be expected to work remotely, but they may occasionally be requested to work on site at the NSPA HQ premises located in Capellen, Luxembourg and must hold a personal SECRET clearance.

The reference number for this contract is IFB-AFSC-PP-2025-056.

BACKGROUND

In early 2024, based on the outcomes and recommendations from industry-led studies assessing the availability and feasibility of potential solutions to fulfil the AFSC Capability Requirements, the North Atlantic Council approved the AFSC Technical Concept and its incremental implementation. This concept outlines a vision where surveillance assets, tactical control assets, and effectors can connect seamlessly and respond dynamically to changing operational situations and where manned and unmanned systems are able to act in synergy leveraging manned-unmanned teaming capabilities. This AFSC System of Systems will be able to operate across all environments, from benign, to contested, and into denied battlespace, ensuring a lower risk to the manned assets.

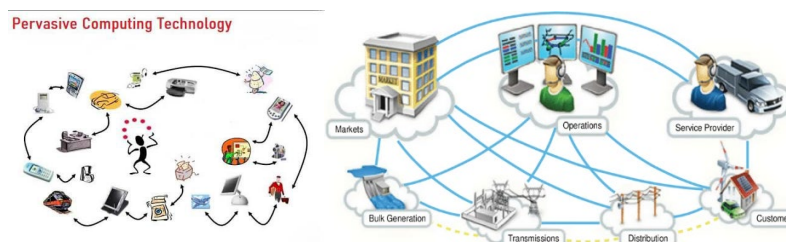
The expected retirement of NATO's Airborne Warning and Control System (AWACS) fleet around 2035 led NATO to initiate the AFSC Concept Stage with the aim to define a new generation of surveillance and control capabilities. Based on the outcomes and recommendations of studies conducted in the Concept Stage, NSPA has defined an AFSC Technical Concept for a distributed multi-domain Battle Management Command and Control (BMC2) and wide-area surveillance system of systems employing a wide range of systems and platforms integrated through a robust and adaptive interoperability architecture to allow a variety of flexible system configurations in future multi-domain operations. Following the anticipated completion of the AFSC Concept Stage in December 2025 will be an immediate start of the Development Stage in January 2026

DATA CENTER DISSENSION

Why do we need these additional “drone swarm ambient computer” helpers outside people’s houses?

<https://lbsitbytes2010.wordpress.com/2013/03/20/pervasive-computing/>

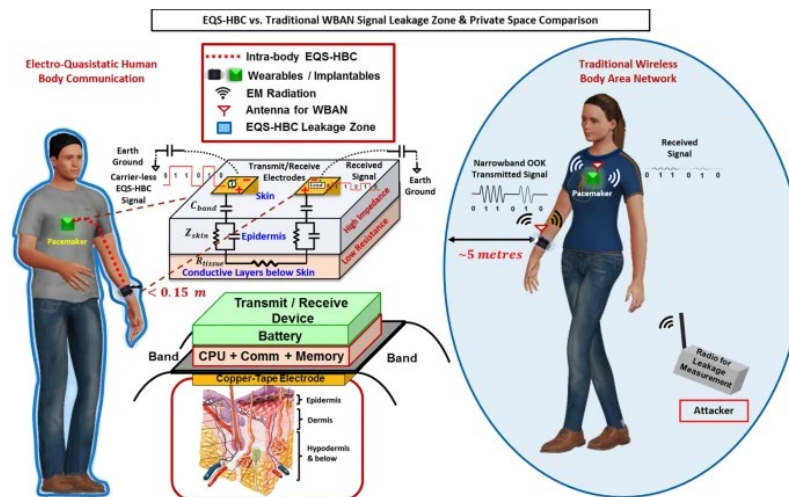
Pervasive computing (also called ubiquitous computing) is the growing trend towards embedding microprocessors everyday objects so they can communicate information. The words pervasive and ubiquitous mean “existing everywhere.” Pervasive computing devices are completely connected and constantly available.



<https://www.sciencedirect.com/topics/computer-science/pervasive-computing>

Pervasive computing refers to the concept of creating ambient intelligence through networked devices embedded in the environment, providing unobtrusive connectivity and value-added services to enhance human experience and quality of life without explicit awareness of the underlying technologies.

<https://www.wiley.com/en-us/shop/general-introductory-computer-science/fog-edge-and-pervasive-computing-in-intelligent-iot-driven-applications-p-9781119670100>



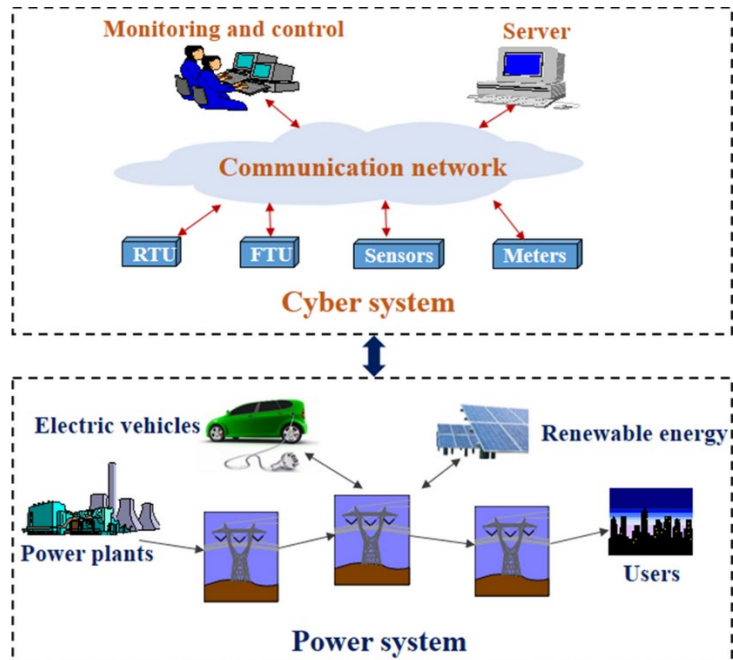
Cyberphysical to WBAN

<https://www.mdpi.com/1424-8220/23/17/7391>

https://www.researchgate.net/figure/Examples-of-cyber-physical-systems_fig1_346986587

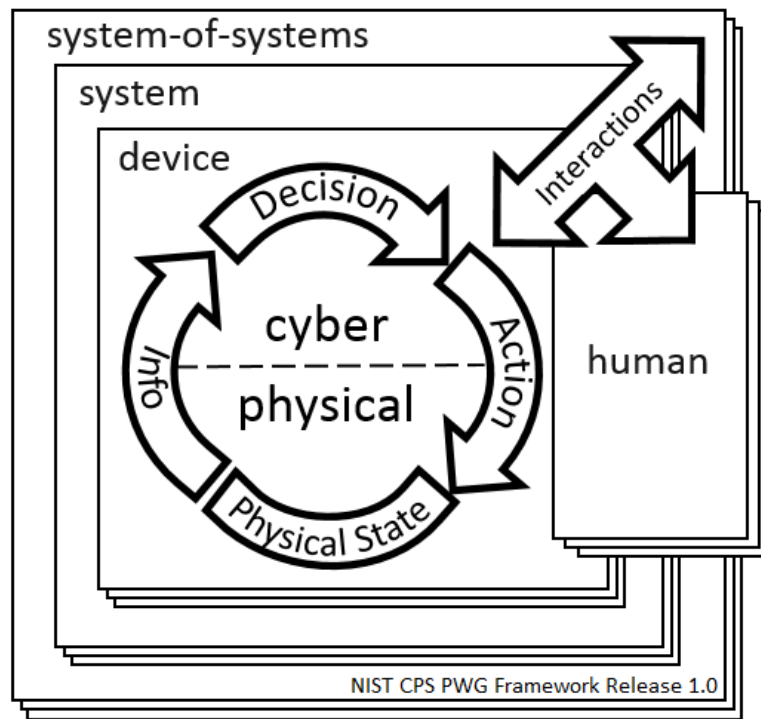
Cyber-Physical Systems (CPS)





Architecture of a CE-CPS: The integrated system consists of a plant, sensors, actuators, and a cloud-based controller. The cloud-based controller is composed of a local controller, a wireless network, and a cloud. The network is deployed to transmit data of computations to the cloud and the control solutions from the cloud. The controller aims to stabilize the plant and achieve system objectives

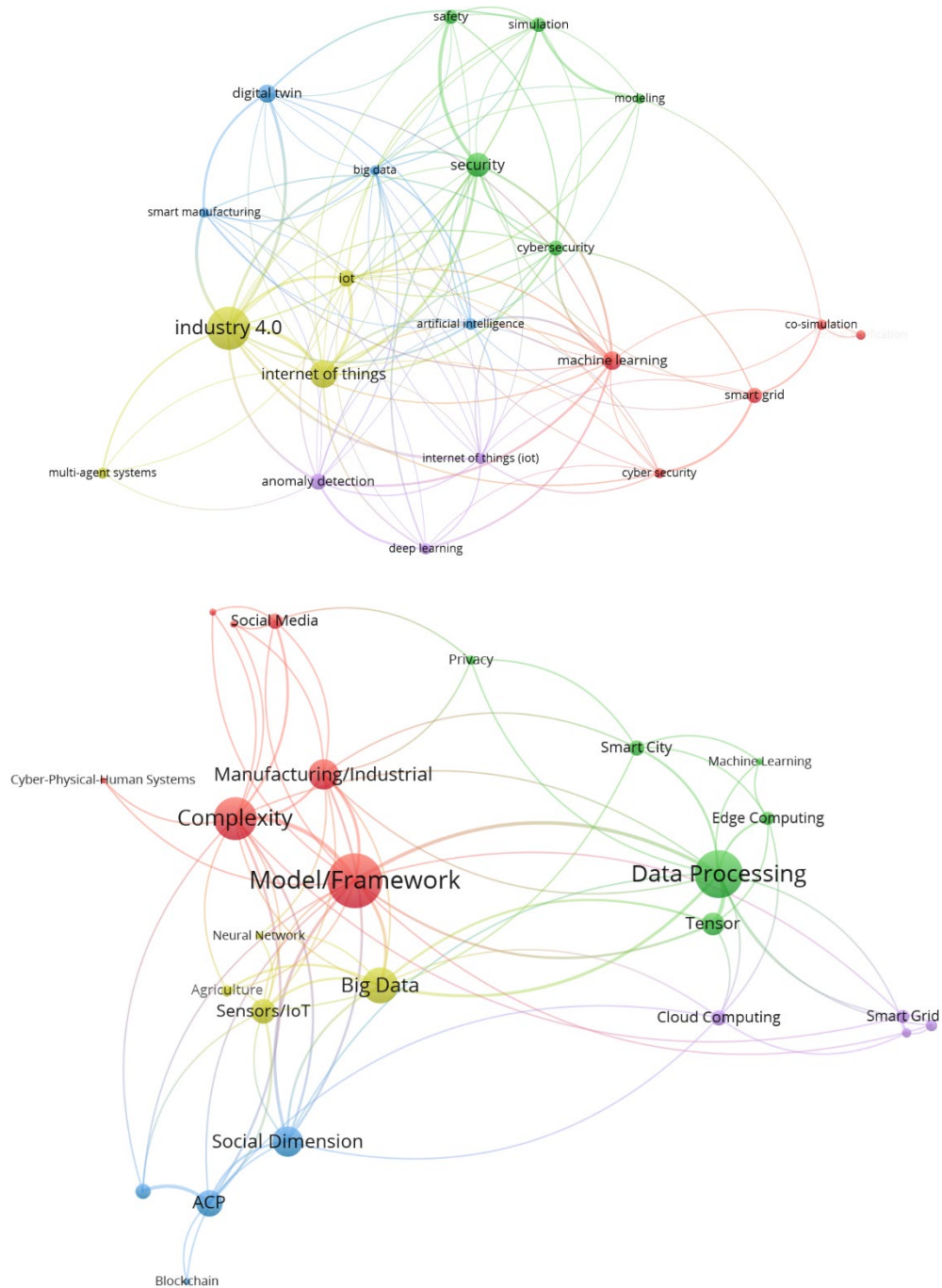
<https://pages.nist.gov/cpspwg/>



<https://pmc.ncbi.nlm.nih.gov/articles/PMC4244980/>

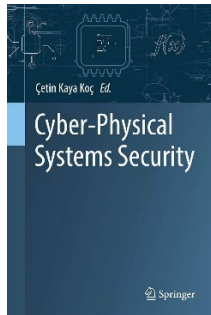
Interference Mitigation for Cyber-Physical Wireless Body Area Network System Using Social Networks

Wireless body area networks (WBANs) are cyber-physical systems (CPS) that have emerged as a key technology to provide real-time health monitoring and ubiquitous healthcare services.



<https://pmc.ncbi.nlm.nih.gov/articles/PMC7909758/>

<https://www.amazon.com/Cyber-Physical-Systems-Security-%C3%87etin-Kaya/dp/3319989340>



Golden Dome PDF -

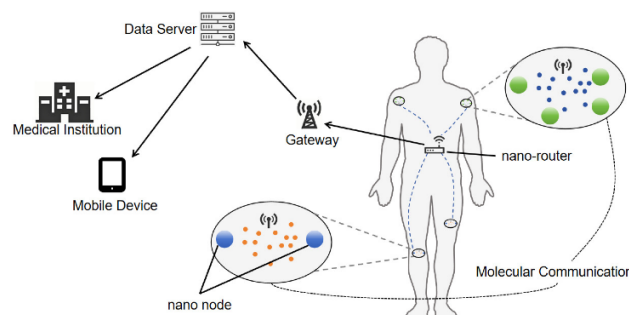
WE MUST DEFEND OUR PEOPLE WITH COGNITIVE WARFARE BECAUSE C40.ORG IS ALREADY PHYSICALLY IN PROCESS.

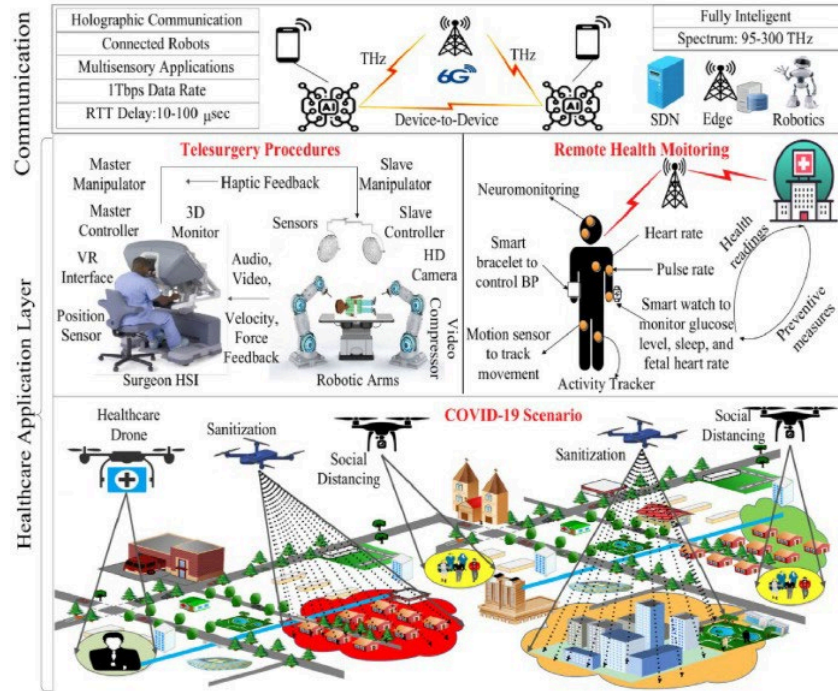
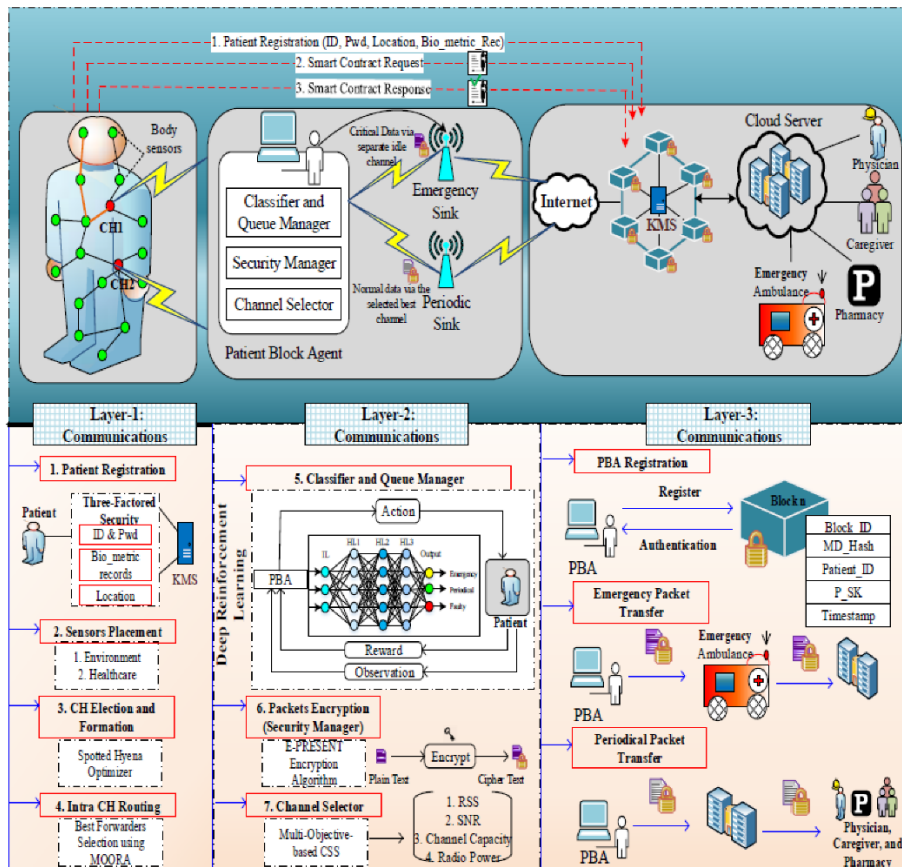
<https://standards.ieee.org/ieee/802.15.6/10941/>

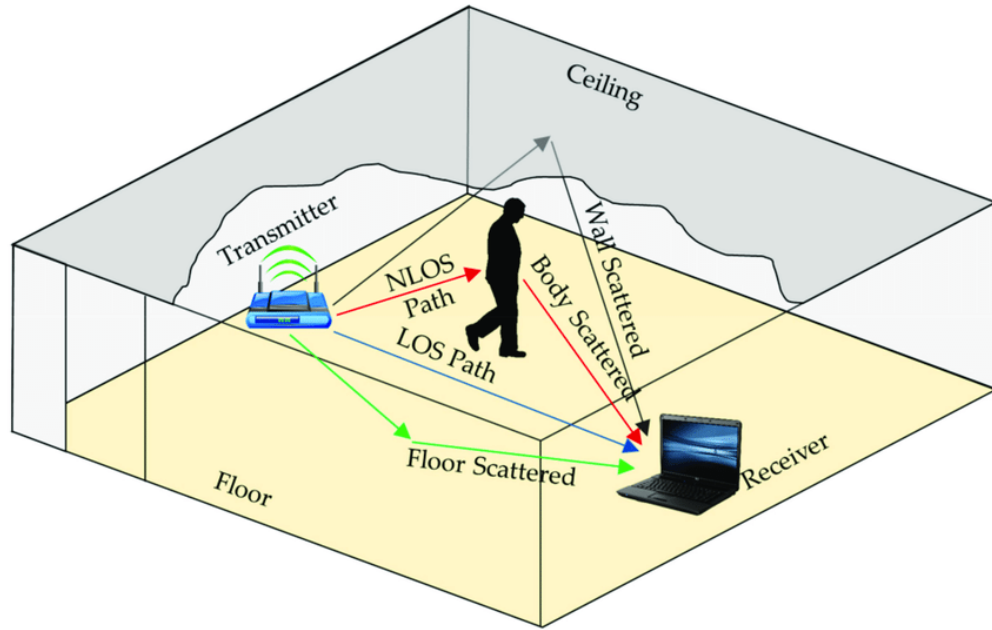
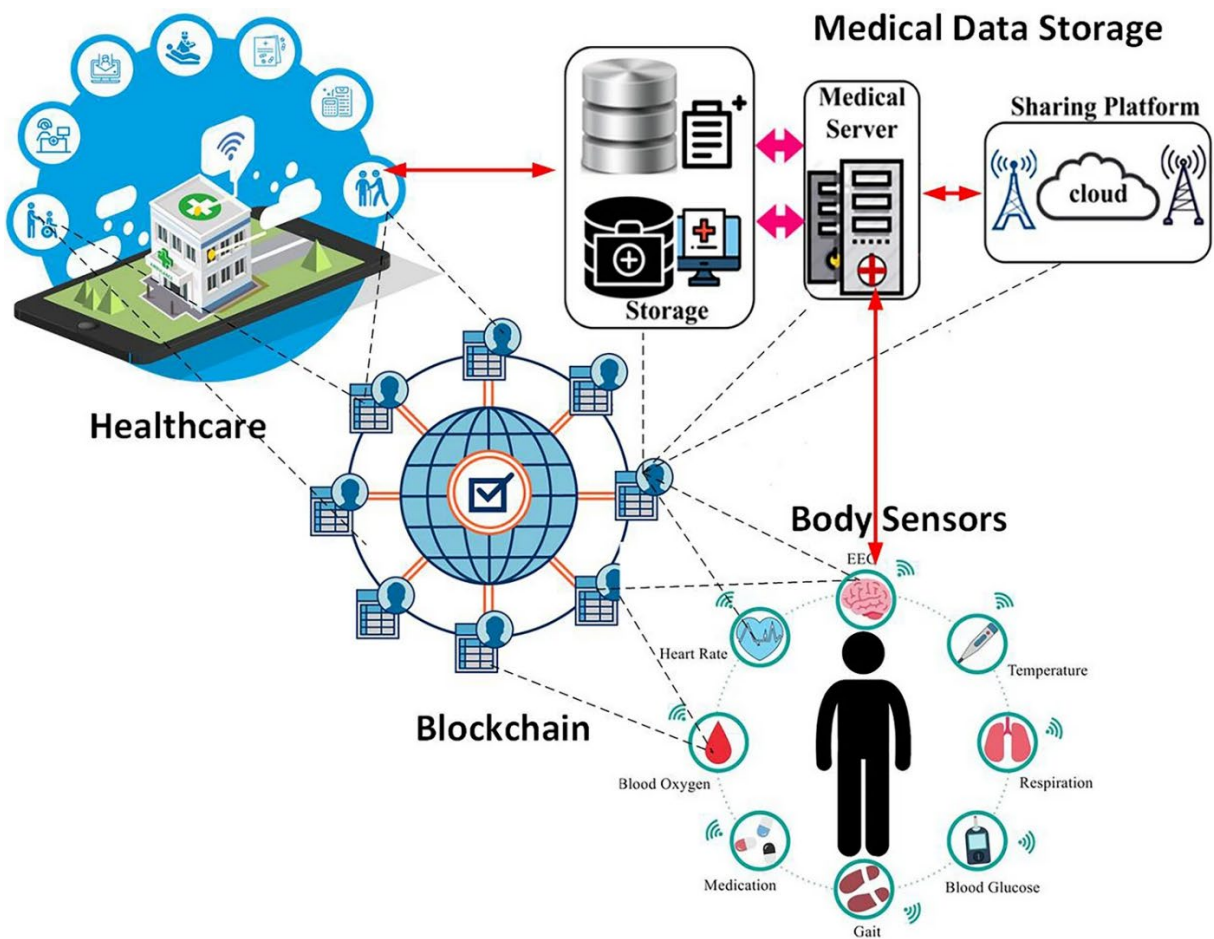
<https://ieeexplore.ieee.org/document/7033222>

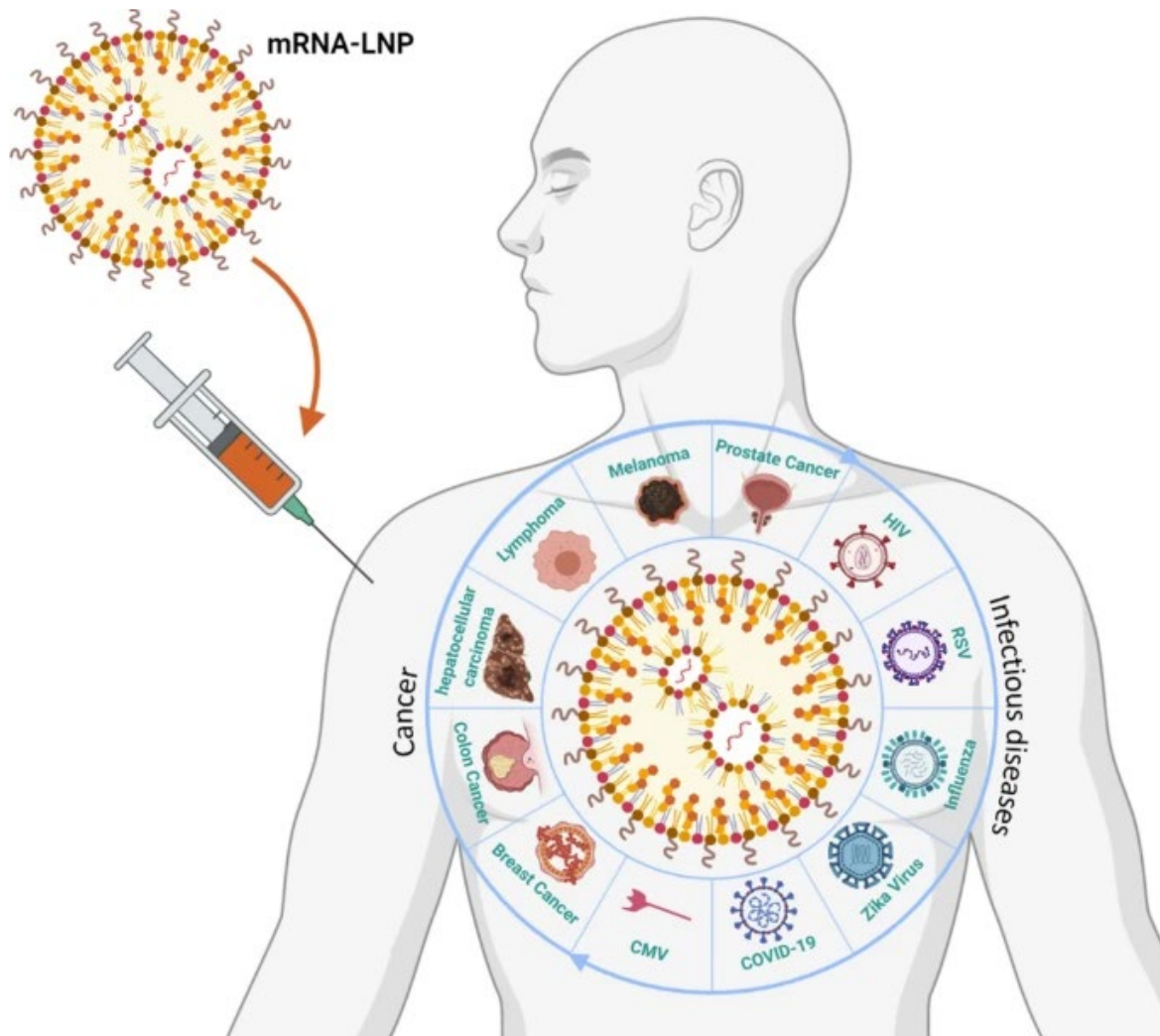
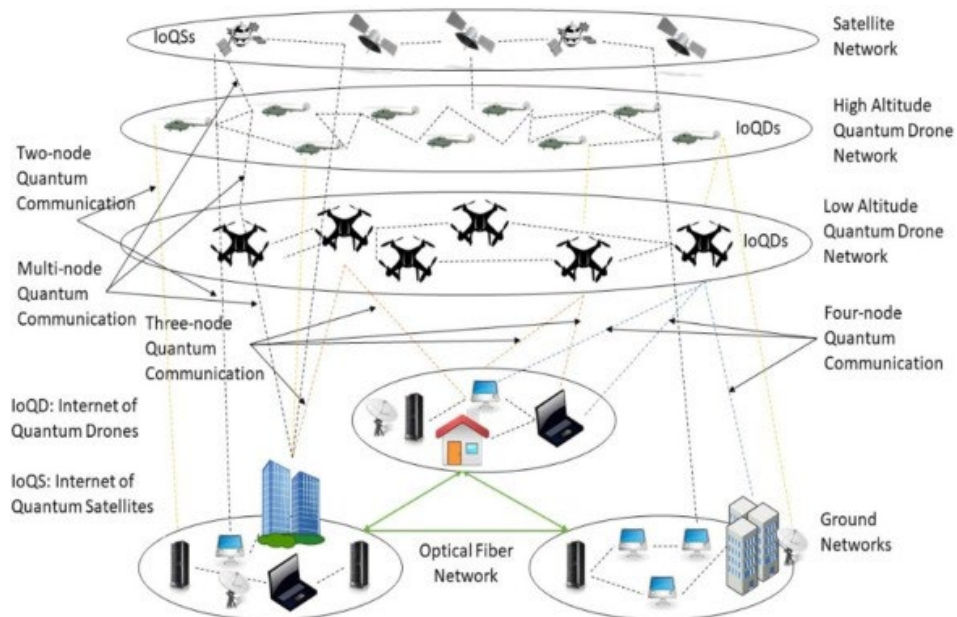
2014

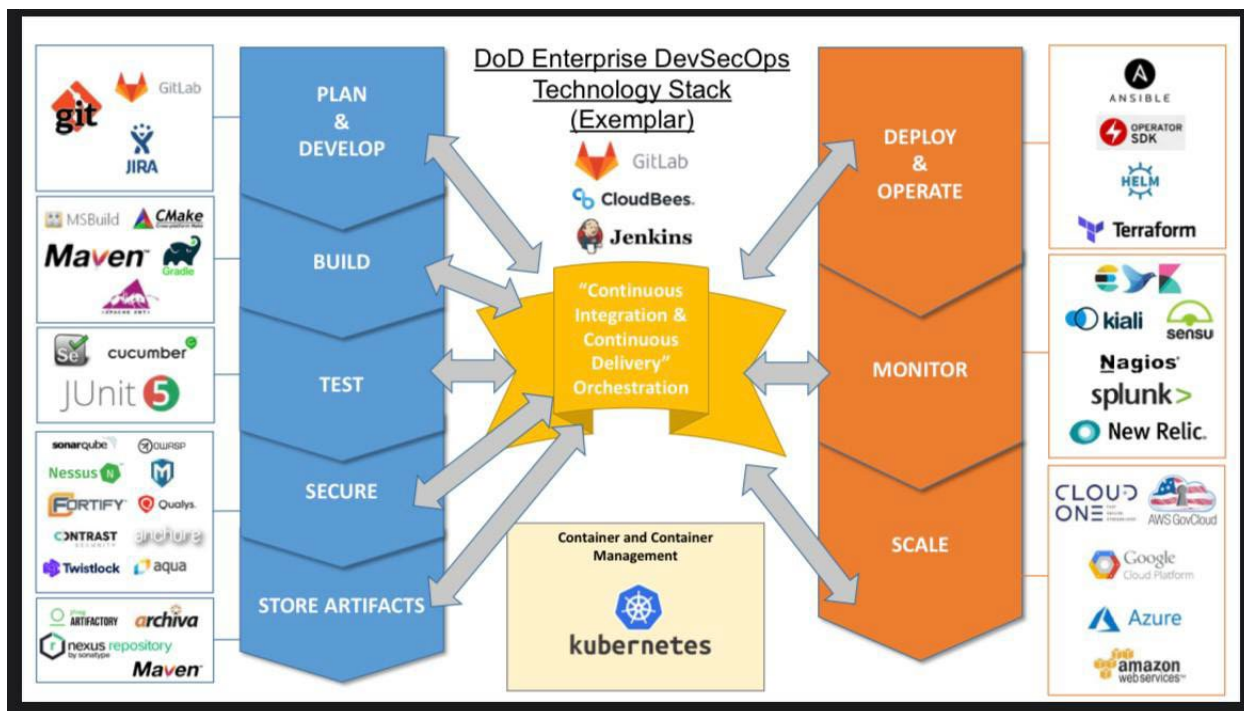
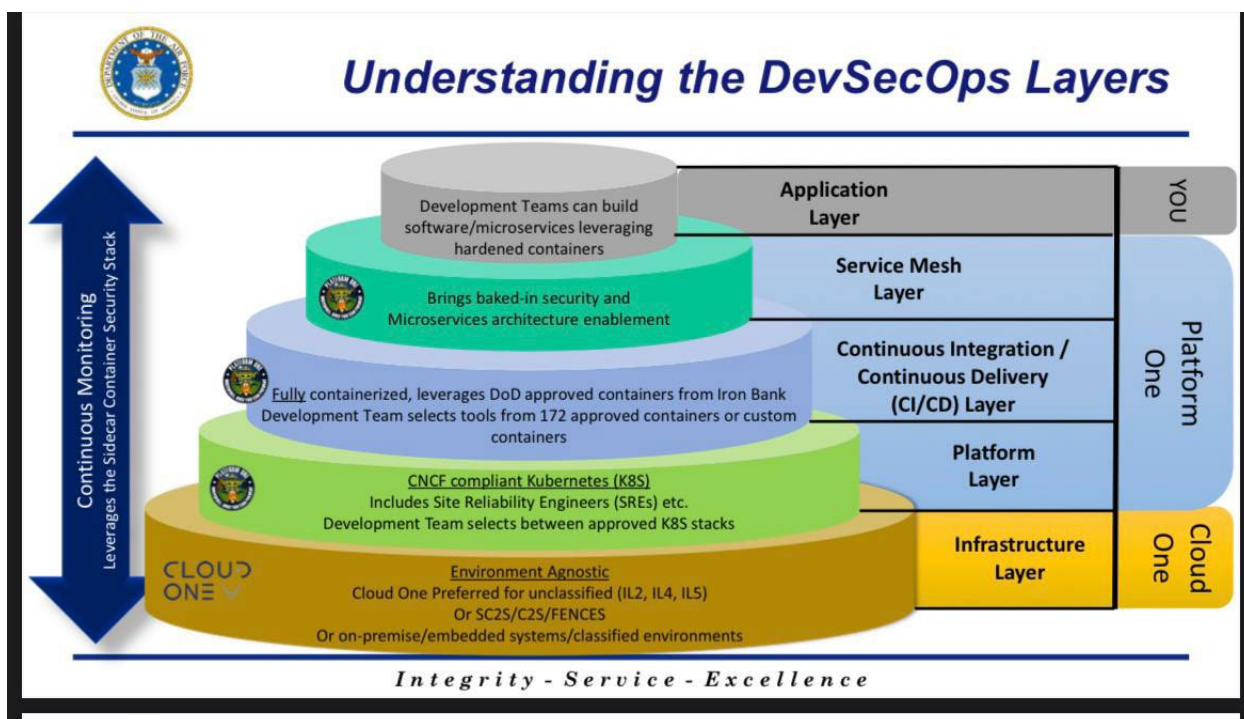
Short-range, wireless communications in the vicinity of, or inside, a human body or vehicle body (but not limited to humans and vehicle) are specified in this standard. It uses existing industrial scientific medical (ISM) bands as well as frequency bands approved by national medical and/or regulatory authorities. Support for quality of service (QoS), extremely low power, and data rates up to 50 Mbps is required while simultaneously complying with strict non-interference guidelines where multiple BANs are coexisting. This standard considers effects on portable antennas due to the presence of a person (varying with male, female, skinny, heavy, etc.), radiation pattern shaping to reduce the specific absorption rate (SAR) into the body, and changes in characteristics as a result of the user motions.











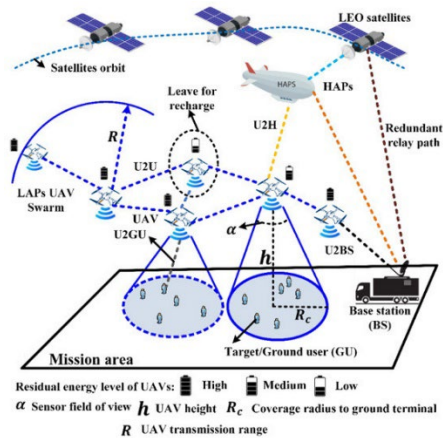
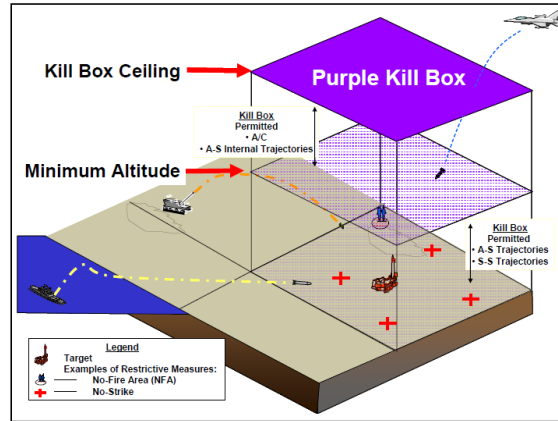
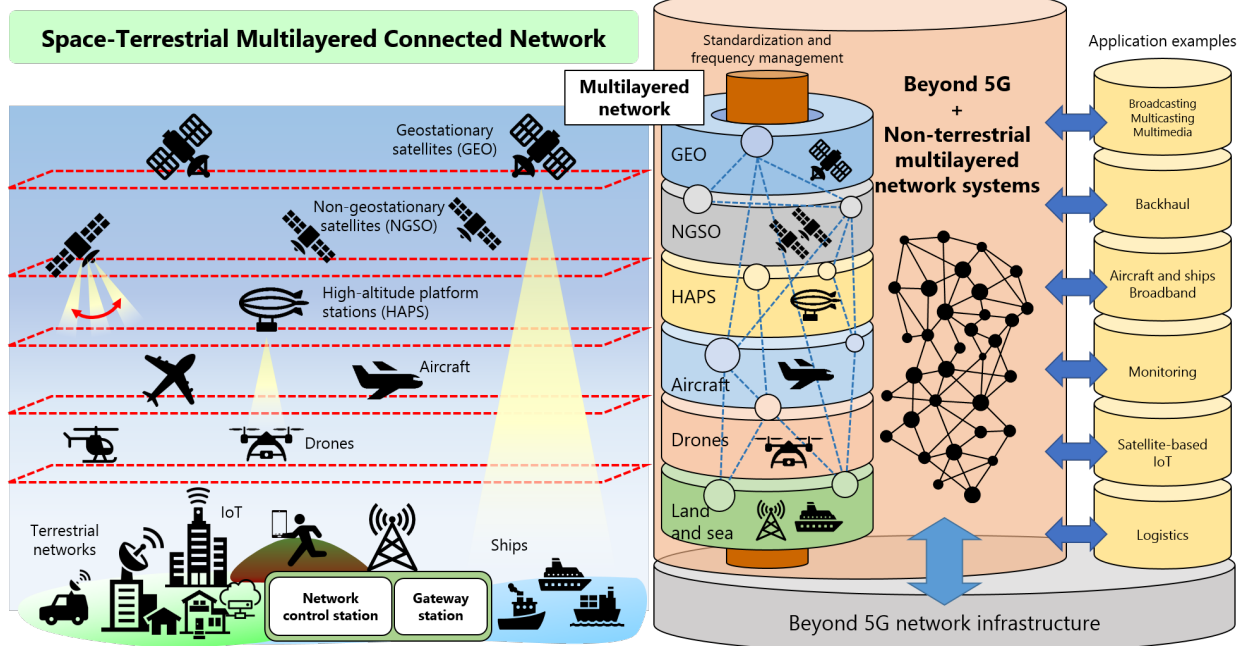


Figure II-2. Notional Purple Kill Box



<https://www.cisa.gov/safecom/NCSWIC>

National Council of Statewide Interoperability Coordinators

Related topics:

[Emergency Communications](#) , [Emergency Communications Coordination](#) , [Emergency Communications Planning](#)

- [NCSWIC Committees](#)
- [NCSWIC Membership](#)
- [SAFECOM, NCSWIC, and Joint In-Person Meetings](#)



Established by the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) in July 2010, the National Council of Statewide Interoperability Coordinators (NCSWIC) supports Statewide Interoperability Coordinators (SWIC) from the 56 states and territories, by developing products and services to assist them with leveraging their relationships, professional knowledge, and experience with public safety partners involved in interoperable communications at all levels of government.

CISA is the lead coordination agency for the NCSWIC and recognizes the critical role the SWICs serve in organizing and executing the interoperability effort in all the states and territories.

<https://tore-says-show.simplecast.com/episodes/mon-07-feb-first-domino-evil-moves-j6-fraud-slow-unity-vaxugenics-djt-nuggets-queen-2-f7?t=1h45m55s>

Episode Summary

Every move they make is destructive to America. What happens when the thumb is off the scale? What is taught today isn't real history. Our unity as a people will pull us through. Flu versus Covid. Fake data, scary peaks, coding tweaks and whistle blowers. VAX experiments in Africa and population control. US aid is gone \$\$\$\$. The first domino makes the rest fall. Is that you Warren? You can't lock them ALL up. Without valid ID, we have nothing. As tech evolves, so must our privacy. Where's Durham? Hints flow as our President interviews with Kash Patel. Raskin ethics. Before the big moves, it all has to be perfect. Adding insult to injury. Demons crawl in thru open borders. It is what it is for now, because sometimes things are a little bit different.

22

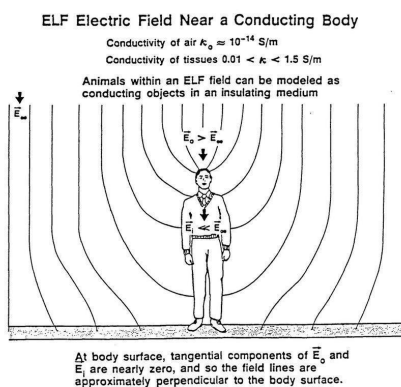


Figure 2

<https://www.osti.gov/servlets/purl/6904679>