Potential advantages of cognitive sensor-to-effector loops (CStELs)

Paul Labbé, Defence Scientist, IEEE Life Senior Member
Defence Research and Development Canada (DRDC), Ottawa, Ontario, Canada, K1A 0K2
Paul.Labbe@drdc-rddc.gc.ca

Abstract

This paper examines the potential advantages of a cognitive sensor-to-effector loop (CStEL)[1], or 'cognitive sensor-to-shooter loop' (CStSL), concept over a non-cognitive one. The concept results from the author's research on cognitive radars (CRs) and internet of intelligent things (IoITs). Also this paper contributes to his current research on cognitive radio network (CRN) in support of Defence Research and Development Canada (DRDC) science and technology (S&T) outlook to inform our organisation and the Canadian Department of National Defence (DND) about the potential operational impact of such technology advances. The envisaged CStEL is assumed to rely on intelligently internetworked cognitive components such as cognitive IoIT ecosystems which include sensors and effectors such as CR, cognitive electronic warfare (CEW), cognitive weapon (CW) such as cognitive missile or cognitively optimised directed energy weapon (CODEW) and CRN. According to literature surveyed, in some instances, CRs may offer improvement (gain) by one-order of magnitude in timeliness, accuracy and detection range which represents significant advantages to early adopters. Being at the cusp of practical specialized artificial intelligence (AI) in small devices which is critical to the CStEL concept, one may hypothesise that such CRs gain could be attained by CWs and by the cognitively supported decision process of CStEL, thus to expect that the overall system may offer one-order of magnitude in improved interception rate success (positive outcomes of engagements). All of this can be seen as a result of significant progress of low power demand technologies advancing specialized and general AI. This means less human (cognitive) intervention in the loop for local analytics which ensures speedier CStEL with more useful timely and actionable information to be shared.

Keywords: cognitive sensor-to-effector loop (CStEL), cognitive sensor-to-shooter loop (CStSL), Internet of things (IoT), cognitive radar, cognitive network, cognitive radio, internet of intelligent things (IoIT), internet of battlespace things (IoBT), internet of military things (IoMT), jamming, artificial intelligence (AI), analytics, track data, emerging technology, efficiency, 'command, control, communications, computers, intelligence, surveillance and reconnaissance' (C4ISR), intercept, missile, directed energy weapon, sensor and effector.

[1] This is related to the known 'sensor-to-shooter loop' but here we add cognition so it could be labelled as 'cognitive sensor-to-shooter loop' (CStSL). The author selected the word effector to include softkill techniques and evasive defence systems.

[1] P. Labbé, "Model-based Measures for Over-the-horizon Targeting with Improved Sensor-to-shooter Timeliness," in *1999 Command and Control Research and Technology Symposium; Change and Continuity in the Future of Command and Control*, U.S. Naval War College, Rhode Island, 1999, p. 23: Department of Defense Command and Control Research Program (DoD CCRP).

1. Introduction

During a literature review of material on cognitive radar (CR) I noted an alternative to the well-known observe-orient-decide-act (OODA) cybernetic loop used in command and control. In an article by Guerci [2] on advanced CR an additional step was added for prediction which is also reported in a Naval Postgraduate School (NPS) report by Camacho *et al.* [3]: observe-orient-predict-decide-act (OOPDA) loop. The OOPDA is similar to cybernetic models used by the author [4, 5] in analysing coalition live and simulated exercises where the decision-making processes at command centers can be interpreted as a cognitive adaptive-control system including the following activities (changes in parameters in this kill chain allow to compare legacy systems as sampled to a perfect one or one with AI, i.e., the 'cognitive sensor-to-shooter loop' (CStSL)):

1- monitor the situation;
2- assess the situation and estimate adversarial intent;
3- develop alternative course-of-action (COA);
4- predict their consequences for both sides (own and opposing forces);
5- decide a COA; and
6- direct its execution while monitoring the evolving situation in the environment (cycle 1 to 6).

Furthermore, the model must interact with external processes and agencies to inform and query, through direct and remote monitor functions respectively. In such cybernetic models, the decision making processes recursively steps through a six-stage cycle. By using cybernetic models to interpret data and information collected during experiments, one can execute and evaluate the stages through a set of measures of performance (MOPs). Similarly, measures of effectiveness (MOEs) can provide an assessment of the resulting degree of mission accomplishment in scenarios to scale MOPs relatively to MOEs.

Advances in spectrum efficient, cognitive sensor networks, radio geolocation and energy conservative cognitive radio networking (CRN) are well documented in the literature including some work done in support of the Canadian Armed Forces (CAF) [6-16] and one on high frequency (HF) CR [17]. The media access for non-primary users with optimal spectrum use under low energy regime is exemplified by the sense and predict strategy documented in [18]. A typical cognitive sensor-to-effector loop (CStEL) could be built using a communication cloud enhanced by cognitive components which optimised channel capacities as function of the activity supported such as orderwire versus high speed data transfer between CRs. The orderwire is a high-priority channel used to manage network components which usually requires only small amount of data transfer but highly critical to ensure a dependable service. On the other hand, raw signal data exchange between two radars for improving track continuity and target detection by correlating multiple signals requires a high throughput for a large amount of data but could accept sporadic data loss and interruptions with low impact on the overall performance of the tracked target when using appropriate processing, prediction and management.

This concept paper will bring some evidences of the potential gain of early adoption of CStEL on specific decision making outcomes based on previous studies.

2. Difference between adaptive and cognitive systems

Some of the material regarding adaptive and cognitive electronic systems came from the radio communication technology:

"Adaptive systems are defined as being capable of modifying their parameters, including frequency and power, in order to improve the quality of reception. Today, such systems are limited to the medium and high frequency bands, where propagation conditions vary significantly. Regulatory provisions applicable to adaptive systems prohibit their operation in the bands used by safety services, as well as by the radio astronomy, radiodetermination, amateur and broadcasting services. Further technological developments have increased the capabilities of adaptive systems. Software plays an important role in this respect, making it possible to analyse the radio environment and adjust system characteristics to specific operational situations. Such a combination of radio equipment and software offers new solutions for resolving the problem of frequency congestion and improves the overall efficiency of spectrum use. With these technological advances, two new concepts have emerged: software-defined radio and cognitive radio systems[2]".

"Software-defined radio is a radio transmitter and/or receiver employing a technology that allows the RF operating parameters including, but not limited to, frequency range, modulation type, or output power to be set or altered by software, excluding changes to operating parameters which occur during the normal pre-installed and predetermined operation of a radio according to a system specification or standard[3]".

"Cognitive radio system is a radio system employing technology that allows the system to obtain knowledge of its operational and geographical environment, established policies and its internal state; to dynamically and autonomously adjust its operational parameters and protocols according to its obtained knowledge in order to achieve predefined objectives; and to learn from the results obtained[4]".

These concepts have been generalized to systems and neurology science. Now we talk about a new unit, like the bit in communications, the cognit [19]. Figure 1 illustrates a possible representation of a cognitive loop assuming that different types of memory (short and long term) are at play when exercising cognition. The short term memory captures the changes perceived in the observed environment. The long one is used in the reasoning to evolve a new pattern or signal to increase the desired effect or increase an understanding of what happens in the environment.

Haykin [20] stated that: CR "differs from traditional-adaptive radar (TAR) as well as fore-active radar (FAR) by virtue of the following capability: **the development of rules of behaviour in a self-organized manner through a process called learning from experience that results from continued interactions with the environment**." This overarching principle of a CR was based on the ability of bats and dolphins to track and home in on their prey. Long-range detections may require different strategies or principles than those for home in vision optimisation techniques.

[2] https://itunews.itu.int/en/NotePrint.aspx?Note=2076 (Access date: 21 August 2018).
[3] Source: International Telecommunication Union, report ITU-R SM.2152.
[4] Same.

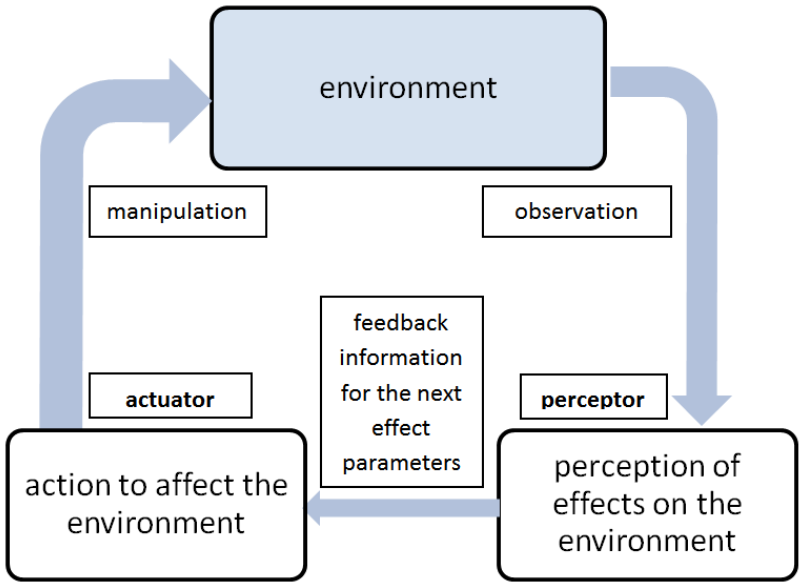

Figure 1 Generic cognitive cycle also known as the sense-learn-act cycle (modified from Haykin [21])**.**

In general an adaptive system reacts to the environment using fix predefined algorithms. A cognitive system in addition can learn from the observed effects from stimulus it designed and generated. It can create new algorithms based on observations of its manipulation of the environment. Cognitive systems are proactive (anticipative or predictive) while adaptive ones are responsive (wait that something happens, they don't probe the environment to see what happens if…).

3. Background, kill chain and CStSL terminology

Here are some excerpts from a NPS report on the subject of accelerating the sensor-to-shooter kill chain [3]: "The kill chain functions were represented in the simulation in the context of the higher-level aggregation of the OODA loop. Uncertainty was represented by statistical distributions of stressor threat inter-arrival and service times that provides predictive forecasting through statistical inference, which was absent from the conventional OODA loop…To reflect uncertainty in the C2 response, the OODA loop needs a prediction function inserted into a revised Observe-Orient-Predict-Decide-Act (OOPDA) loop"[3]. "The measures of performance used in the simulation were the means of the following: the number of IA [information assurance][5] attacks; the number of electronic countermeasures softkills; the number of threat missiles killed by interceptor missiles; the number of re-engagements; and the number of leakers"[3].

"An effective CMD [Cruise Missile Defense] system design requires the achievement of the smallest possible reaction time from threat detection to weapons firing. FORCEnet[6] and OA [Open Architecture] will expedite data flow due to support common services and reduce human interaction in the kill chain. The sensor-to-shooter kill chain can be hastened by introducing automated processes and computational intelligence, using fuzzy logic and neural networks, which in turn will curtail time lost due to organic intervention. Unfortunately, the neural network technology is not

[5] Texts in square brackets are added information to cited texts.
[6] FORCEnet is the operational construct and architectural framework for Naval Warfare in the Information Age which integrates warriors, sensors, networks, command and control, platforms and weapons into a networked, distributed combat force, scalable across the spectrum of conflict from seabed to space and sea to land.

sufficiently mature, but recent research and development with neural networks show promise for the design as well as other adaptive technologies, which can increase system automation and reduce reaction time"[3].

Now a decade later, as mentioned in [22], it appears that we might be at the cusp of practical specialized artificial intelligence (AI) in small devices which is critical to the CStEL concept. The CStEL concept offers a vision of future real-time information systems tailored to command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) system requirements. Future C4ISR will heavily rely on a large number of generic and specialized internet of intelligent things (IoIT) providing some cognitive ability and enhanced agility [23] in complex scenarios.

"The PEO IWS [Program Executive Office of Integrated Warfare Systems] architecture simulation results were the control group in both the raid and the stream cases. The simulation revealed that there was no silver bullet and architecture changes alone will not solve the Navy's ability to counter stressing CMD threats. ASCM's [Anti-Ship Cruise Missile] successfully perforated the defensive layers resulting in leakers in both attack scenarios. Nonetheless, the simulation revealed that the proposed architecture delivered a statistically significant performance improvement compared to PEO IWS's OA functional domain model. Thus, the authors conclude that the proposed architecture should include a re-engagement loop and retain the human in the decide function of the OODA loop"[3].

Again a decade later, one may suggest to use a supervised AI instead of a full-time human in decide cognitive function.

"Situation prediction is an extrapolation of the analyses to a future point in time. It is the projection of the current situation, which is developed by the various situation assessment and evaluation functional sets, into the future [24]. The purpose of situation prediction is to estimate the enemy course of action (COA) and potential impact of the battleforce's planned actions, to predict real-time, near real-time, and non-real-time operational situations." In the development of the model-based-measure (MBM) the notion of predicted position was associated with physics-aware dead reckoning model implemented in Newtonian mechanics [25].

In addition to the main components of CStSL such as CRs one must recognise a large variety of low cost entities, the Internet of Things (IoTs) and Internet of Intelligent Things (IoITs) [22], with self-configuring, adaptive and complex network that interconnects through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. In public security and military scenarios the ubiquitous connectivity cannot be always achievable. This is a significant issue that needs to be addressed for such applications. The evolution of IoT technologies and applications drove specific specialisation and generalisation. For example internet of everything (IoE)[7] is considered a superset of IoT and machine-to-machine (M2M) communication without human interventions is considered a subset of IoT. Examples of specialised IoT includes: internet of military things (IoMT) [26-29], internet of battle things (IoBT) [8, 30-37] and IoIT [38-40]. IoITs are more capable and autonomous things, adding artificial intelligence (AI) and some

[7] https://www.iottechexpo.com/2016/01/m2m/ioe-vs-iot-vs-m2m-whats-the-difference-and-does-it-matter/ (Access date: 20 April 2017).

capabilities of acting without human interventions, so they may have some cognitivity capability. Other authors document tools and prototypes to explore novel ways for human-computer interaction (HCI) with IoT [41]. Some IoT technologies offer better cyber, hacking and security protections due to economic and secrecy of their business, industrial internet of things (IIoT) [42-47]. In fact [48] extends IIoT technologies to public safety and defence.

Adding AI to intelligent communication networks contributes to their adoption in fields like healthcare, military or prediction of seismic activity in volcanoes [40]. Distributed intelligence adds benefits such as no single point of failure, provides local users with more real-time information and reduces load and traffic to centralized computing. The centralized system helps providing global contexts to local computing which contributes to the coherence of local awareness pictures to a common operating picture (COP) without reducing significantly the timeliness of the local picture.

3.1 Specialized artificial intelligence

Several success stories about AI capabilities have been reported over the last decade including studies on the implications of specialized AI [49-54]. For example, once deeply trained at recognising indicators of a type of cancers from a representative imaging data set, a specialized AI demonstrated its abilities to assess large number of such cancers from other imaging data sets that included some imaging data without this type of cancers with no false detections. Then the AI system was able to find cases of the same type of cancer that were not detected by specialists/experts. However it appears that deep learning neural networks and other AI approaches were using large computing capabilities. Currently this is changing according to an IEEE Spectrum post by Katherine Bourzac [55] since engineers are developing specialized hardware for energy-efficient AI. These will be timely addition to the world of IoITs. Then Bourzac added [55]: "Compared to other algorithms, neural networks require frequent fetching of data; shortening the distance this data has to travel saves energy. Guiseppi Desoli, a researcher at STM's Cornaredo, Italy, outpost, presented a neural network processor that can perform 2.9 trillion operations per second (teraops, 10^{12}) per watt." Not sufficient yet since this means only an hour on a smart phone battery: "only a few teraops per watt".

4. Effectors

As explained in the footnote to the abstract, effector was selected instead of weapon to expand the system beyond hardkill to include softkill interventions such as electronic countermeasures (ECM), jamming, electronic warfare (EW) and its cognitive version CEW [56-60]. Then the defence system could demonstrate its electronic combat effectiveness with an EW softkill as simulated in [3]. For hardkill and softkill, predicting outcomes against threat targets requires comparing COAs and their time lines. Most of the times there are no silver bullets against threats and alternative actions need to be pre-planned. Fleetingness, the fact that actions happen over a very short time, requires anticipating that one countermeasure or missile interception may fail. Using some prediction techniques helps to build the sequence of actions required to attain a high degree of confidence of successfully intercepting the threatening target(s).

If the effector is a hardkill type like a missile with specific characteristics (cognitive or not) for successfully homing in on a target, then these characteristics specify the minimum track quality for valid engagement. In the case of smarter missile with some cognitivity and autonomy, that would be

different and difficult to predict the outcomes. Another aspect is the railgun. A US Navy projected 64 MJ railgun may require 16 MW for 6 MA peak at a shooting pace of 6 shots per minute with a maximum range of 350 km. Such railgun would shoot 10 times further than normal ship mounted guns (a definite advantage in combat) and save a lot of money (improving sustainability) for its operation per shot compared to current guns + ammunitions and missiles.

Laser type of effectors usually need more time to lock on a target due to their narrow beam but their time to reach the target is almost immediate compare to a missile. Jammers, EW and cognitive EW (CEW) offer similar performances at the speed of light [24, 56-60] but don't need to lock on a target so they offer immediate effect or distraction.

4.1 Directed energy weapon (excerpted from [61])

Directed energy weapon (DEW) technologies (these include technologies such as: high energy laser (HEL), radio frequency (RF) DEWs, and relativistic particle beams (RPBs) and high power microwave (HPM)) require usually large and heavy high power sources although technologies advanced made them more deployable. However, such electricity demand still represents a major challenge to accommodate, especially on legacy platforms. Various types of DEWs are currently in deployment phases for air, land and naval platforms with a large variety of electrical energy demands. Figure 2 shows that the pulse power depends on type of targets, use and range.

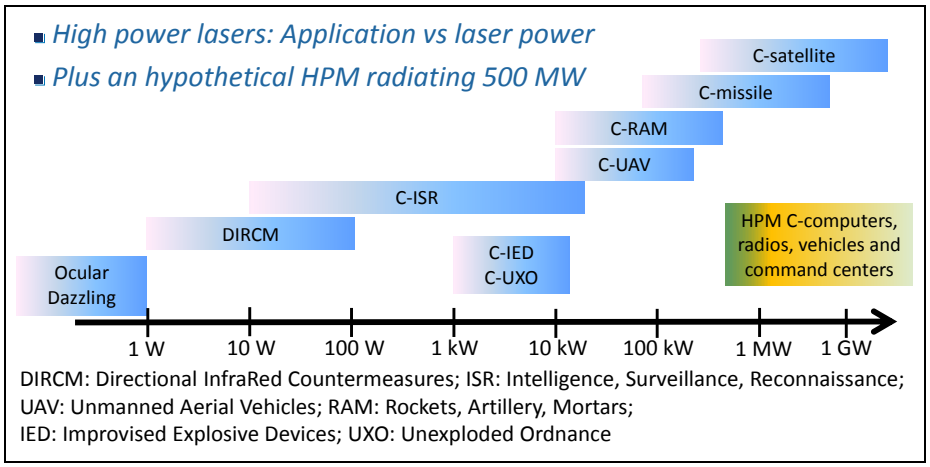

Figure 2 Typical radiating power required for specific counter attack (adapted from [62]).

For an hypothetical HPM [63], the authors assume an efficiency similar to radar technologies, i.e., 17% of the input power results in radiating power. They consider that 3.7 GW of input power is required to deliver, at a range of 10 km, a power flux of 10 kW/m^2 on a 30 mrad spot size of 300 m. References [64, 65] provide information on damage level of DEWs.

It is critical to recognise that these technologies, directed energy weapons, are power hungry while persistent surveillance and C4ISR ones are energy hungry.

4.2 Jammer

Typical jammer capabilities from Figure 3 allow devising an even better jammer strategy by deducing the type of protocol and error correction capabilities of the communication to disturb, this is protocol jamming. Reading reference [66], we find that the authors' intent of the jamming taxonomy paper is "to help researchers place newly discovered jamming or anti-jamming strategies within a larger context of known strategies in a way that is consistent with modern electronic warfare." The authors refer to the Common Attack Pattern Enumeration and Classification (CAPEC)[8] which "is a catalog and taxonomy of cyber-attack patterns, created to assist in the building of secure software. Each attack pattern provides a challenge that the attacker must overcome, common methods used to overcome that challenge, and recommended methods for mitigating the attack." For example, performance improvements in terms of energy efficiency, data streaming speed and accuracy require using system and network self-awareness at various layer levels of the IoT stack [67-73] in order to counter interference or jamming, These networks may share quality of service (QOS) information about the receiving spectrum as seen by the wideband front end of their SDR from each participant location.

A jammer can have one or more of the following major capabilities: time correlated, protocol-aware, ability to learn and signal spoofing.

When a jammer has no knowledge of the protocol to be defeated, it may use digital radio frequency memory (DRFM) jamming (a.k.a. repeater jamming or follower jamming) in the simplest form of correlated jamming. Also it can estimate the automatic gain control (AGC) time constant of the receiver to be jammed.

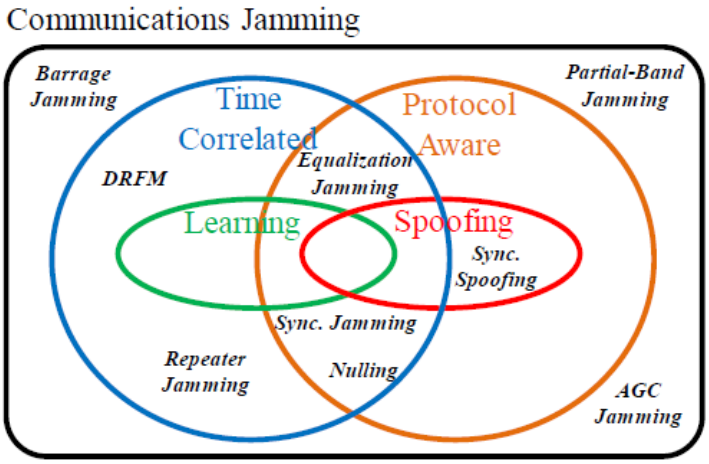

Figure 3: Specific jamming techniques discussed in literature, mapped according to key jammer capabilities (Illustration from [66])[9].

More information about radio communication jamming and network security could be found in [66, 74]. In addition we have to consider the significant research and findings on self-healing networks and sensor networks [13, 15, 32, 74-82] which offer an adaptive approach to counter jamming, adverse propagation, interferences and noise.

[8] https://capec.mitre.org (Access date: 22 April 2017).
[9] With the permission from the authors; Labbé-Lichtman, 3 April 2017.

Next we have to consider the information security (INFOSEC) and communication security (COMSEC) aspects assuming that attacks are within the internetworking. In such cases encryption, randomization and utilisation of blockchain should be sufficient to protect the information. Also this creates a big challenge in managing crypto keys over a large number of IoITs via wireless links [83-85]. Other studies show techniques to increase security at the physical layer (PHYLAW) [47, 86-88].

5. Wireless technologies

Under the hood of the radios of some advanced IoT hardware platforms one finds technologies developed for defence such as software defined radios (SDRs) which evolved under the US Department of Defense (DoD) Joint Tactical Radio System (JTRS) program[10]. Silicon industry, e.g., National Instruments (NI)[11] (Figure 4), looks beyond today best SDR solutions which evolved from field programmable gate-array (FPGA), radio frequency integrated circuit (RFIC) and digital signal processing (DSP) devices in support of military communications (MILCOM), electronic warfare, signals intelligence (SIGINT) and Fourth Generation (4G) phones. Future technologies integrating analog with digital circuits will support IoT and Fifth Generation (5G) smart phones, and other systems yet to be defined.

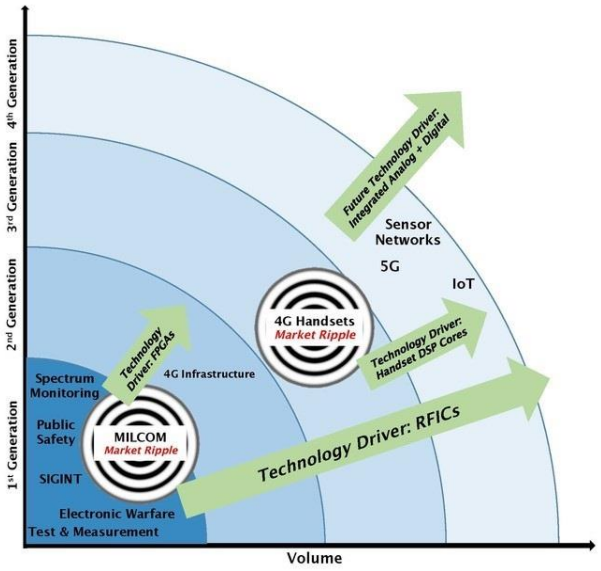

Figure 4 Successive generations of software defined radios have come to dominate the radio industry and will continue to evolve[12].

[10] JTRS was a family of software-defined radios that were to work with many existing military and civilian radios. It included integrated encryption and Wideband Networking Software to create mobile ad hoc networks (MANETs).
[11] http://www.ni.com/white-paper/53706/en/ (Access date: 11 April 2017).
[12] http://www.ni.com/white-paper/53706/en/ (Access date: 11 April 2017). NI copyright permission duly signed on 24 April 2017 for Paul labbé to use this illustration.

6. Example of a cognitive socio-sensing system

In this example from a 2018 IEEE Communication Magazine paper by Ding *et al.* [89], the authors describe an amateur drone surveillance system using cognitive IoITs. This paper relates to CStEL in demonstrating cognitive interactions between sensors, weapons/effectors, drones and people jointly contributing to a crowd based surveillance system. The system of Figure 5 manages information such as localisation, control and tracking by generating sequences of location coordinates for identified targets in a context-aware manner.

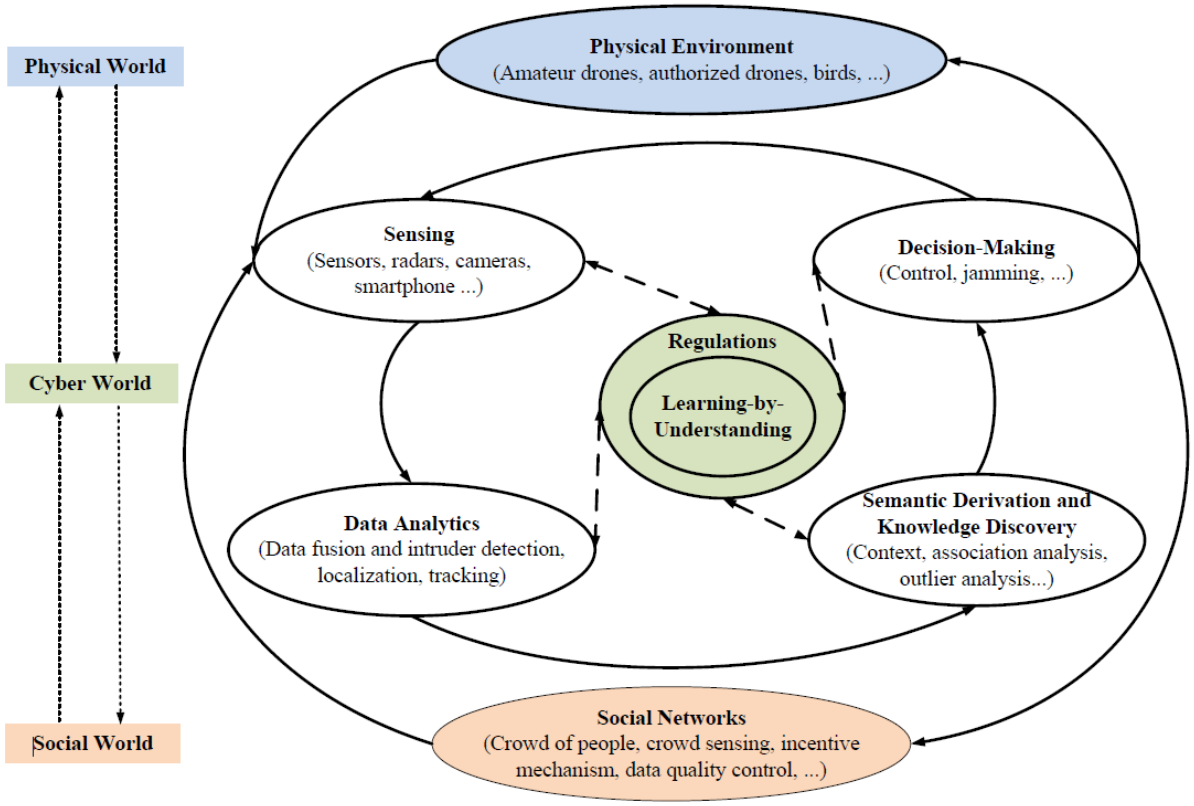

Figure 5 Functional diagram of a cognitively networked amateur drone surveillance system[13].

This system bridges a physical world (physical/virtual things, amateur drones, authorized drones, birds…) and social world (human demand, social behavior…) together as one entity: an intelligent amateur drone surveillance system. It is centered on a synthetic methodology learning-by understanding approach. Its four cognitive tasks are:

1- sensing;
2- data analytics;
3- semantic derivation and knowledge discovery, and;
4- intelligent decision-making.

The system can detect, jam, capture or destroy targets.

[13] With the permission from the authors; Labbé-Ding, 31 July 2018.

7. What happens when human interventions are mainly executed by AI?

When running the MBM cybernetic models over data collected from a large number of trials, we obtain Figure 6 graph relating interception success rate as function of system time delay and track data accuracy. From these trials the main delay was due to the human in the loop and procedures. So if AI is used to accelerate the human process in the loop, the resulting graph shows a steep improvement towards the maximum attainable for a given sensor or track data accuracy.

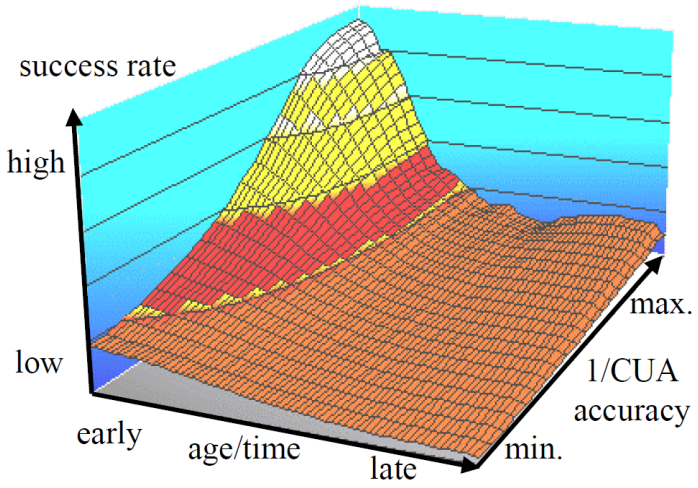

Figure 6 Potential mission success rate as function of input information age and accuracy (inverse of circular uncertainty area, CUA) for a fixed effectors' strategy [4].

Figure 7 illustrates the potential effect of effector broadness (effector's strategy or weapon uncertainty area (WUA)) on interception success rate. If extremely narrow like a laser, the effector will have to lock on the target by searching within the CUA [5].

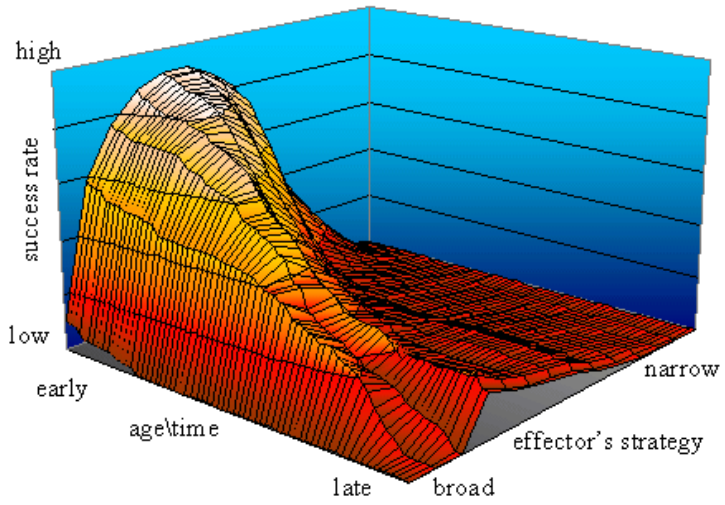

Figure 7 Interception success rate as function of input data timeliness (across available track data accuracy) and effector broadness.

7.1 Cognitive radar (CR) advantage

In the unclassified domain one can find several CR test results from simulations and a few experiments in real environment scenes. In general, the results obtained show significant improvements in all the parameters that radars can provide on a target such as speed, acceleration, distance, altitude and jet engine modulation, and earlier target detection [90]. In most operational scenarios, providing earlier detection time is critical. Some of the reported results showed one order of magnitude better than without the advanced signal processing of CR (performance metric [20] in simulations) or 10 to 15 dB signal-to-interference ratio (SINR) for ground-moving-target indicator (GMTI) improvement against non-homogenous clutter in a real environment using a CoFAR [2].

Figure 8 shows the advantage CR over TAR when using the same signal processing technique, the Cubature Kalman filter (CKF) [91]. The root-mean-square error (RMSE) of the velocity reaches low value much more rapidly for CR than TAR. To reach an RMSE velocity error of about 7.5 m/s CR took 0.17 s and TAR 2.4 s, so more than an order of magnitude faster.

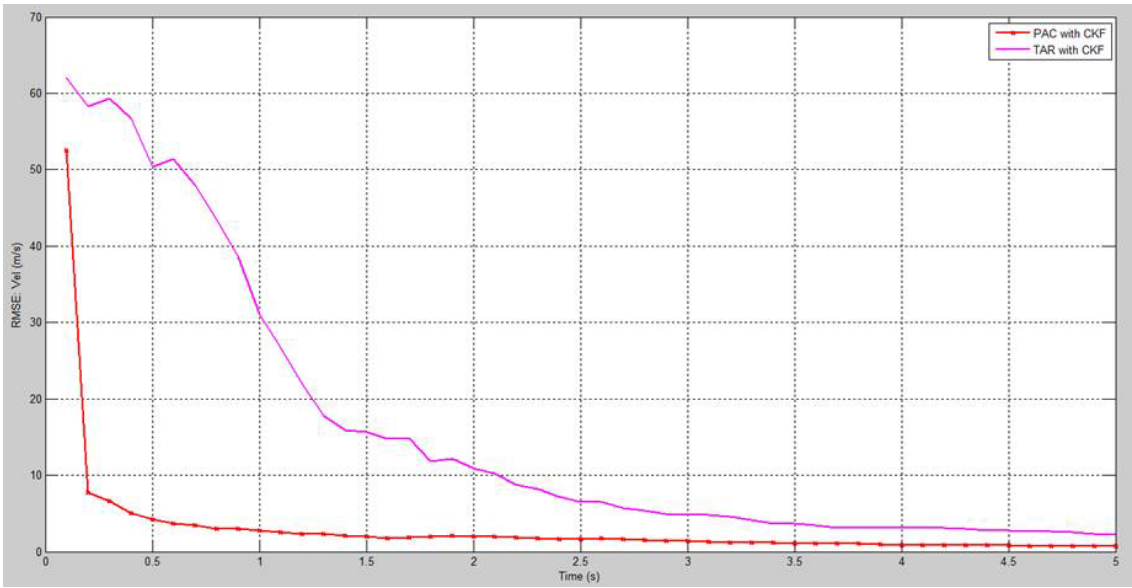

Figure 8 RMSE of Velocity for perception action cycle (PAC)[14] and TAR where both are implemented with CKF[15].

Similar results are provided by Haykin [20, 21, 92-102] that demonstrate improvement in earlier detection of targets with low signal to noise in addition to more precision of the parameters (position, speed, acceleration, bearing, and altitude). Such advantage also leads to earlier prediction of the target intent or allegiance (friend, foe, neutral or civilian).

According to several references on cognitive SONAR (originally an acronym for SOund Navigation And Ranging) [103-106], cognitive technology and associated signal processing and pattern recognition have already proven to be advantageous in underwater operations. Similarly cognitive LiDAR (Light Detection and Ranging) [107-109] provides accurate representations of the environment as applied to autonomous cars.

[14] As for a CR.
[15] With the permission of the authors (10 May 2018 email Labbé-Sarraf).

The development of CR technologies forced an acceleration of cognitive EW technology [56-60] since most traditional EW would not be able to effectively counter the nimble and unpredictable wave patterns of agile CRs. This is claimed to be one of the advantages of advanced fighter aircraft operational systems such as for the F-35 Lightning.

8. Conclusion

From the NPS report by Camacho *et al.* one observes that complementing or replacing some of the human cognitive tasks in senor-to-shooter loops by competent cognition able AI or expert systems, with or without human supervision, a substantial gain in the CStEL (kill chain) is to be expected. In addition by using cognitive sensors, networks and effectors, e.g., CR, CRN and CEW, one expects to see not only cumulative effects of these cognitive components but likely some multiplicative impacts on successful identification tasks, COAs and interceptions. CStEL is accelerating mission effectiveness in complex situations. Furthermore, the author [1] founded similar results using MBMs for over-the-horizon-targeting (OTHT) experiments in estimating the potential gain of sensor-to-weapon loop when accelerating the intervening cognitive human tasks.

Consequently this concept paper shows some evidences (NPS report [3], MBM [1, 4, 5], and CR [20, 21, 90-102]) of the potential gain of CStEL for specific decision making outcomes as from MBM studies of C4ISR system performance during preparedness exercises such as RIMPAC[16].

9. Recommendations

The proposed CStEL concept needs to be evolved in collaboration with experts in several domains and importantly with the communities of end users in order to develop sufficient trust in such cognitive system to use it in operational theaters. In reference [110] they study autonomous weapon systems in terms of learning capabilities from basic machine learning (ML) to learning autonomy. There are other issues such as ethic and accountability of actions for all rules of engagement (ROE).

Decisions errors during autonomous car trials confirm that the evolution of cognitive systems toward trustable AI entities could take more time than what was expected by some of their proponents. This is well documented in the Cutter Business Technology Journal 2018 article by Siau and Wang [111]. There is also a potential susceptibility to cyber-attack which IoIT could mitigate as reported in [22].

10. References

[1] P. Labbé, "Model-based Measures for Over-the-horizon Targeting with Improved Sensor-to-shooter Timeliness," in *1999 Command and Control Research and Technology Symposium; Change and Continuity in the Future of Command and Control*, U.S. Naval War College, Rhode Island, 1999, p. 23: Department of Defense Command and Control Research Program (DoD CCRP).

[2] J. R. Guerci, R. M. Guerci, M. Ranagaswamy, J. S. Bergin, and M. C. Wicks, "CoFAR: Cognitive Fully Adaptive Radar," in *2014 IEEE Radar Conference*, Cincinnati, OH, USA, 2014, pp. 984-989.

[3] J. G. Camacho *et al.*, "Open architecture as an enabler for FORCEnet Cruise Missile Defense," Monterey, California. Naval Postgraduate School, 2007.

[16] RIMPAC, the Rim of the Pacific Exercise, is the world's largest international maritime warfare exercise.

[4] P. Labbé, Z. Maamar, E. Abdelhamid, B. Moulin, R. Proulx, and D. Demers, "Recommendations for Network-and Internet-based Synchronized E-activities for Location-and Time-dependent Information," in *7th International Command and Control Research and Technology Symposium, 7th ICCRTS*, Loews Le Concorde, Québec City, Canada, 2002, p. 27: CCRP.

[5] P. Labbé and Z. Maamar, "Telecommunications Requirements for Nomadic Users of Dynamic Information," in *Winter 2002 La Scuola Superiore Guglielmo Reiss Romoli (SSGRR), SSGRR 2002w,*, L'Aquila, Italy, 2002, p. 10.

[6] O. B. Akan, O. B. Karli, and O. Ergul, "Cognitive radio sensor networks," *IEEE Network*, vol. 23, no. 4, pp. 34-40, 2009.

[7] C.-M. Chen, S.-C. Hsu, and G.-H. Lai, "Defense Denial-of Service Attacks on IPv6 Wireless Sensor Networks," in *Genetic and Evolutionary Computing: Proceedings of the Ninth International Conference on Genetic and Evolutionary Computing, August 26-28, 2015, Yangon, Myanmar - Volume 1*, T. T. Zin, J. C.-W. Lin, J.-S. Pan, P. Tin, and M. Yokota, Eds. Cham: Springer International Publishing, 2016, pp. 319-326.

[8] G. Hua, Y. X. Li, and X. M. Yan, "Research on the Wireless Sensor Networks Applied in the Battlefield Situation Awareness System," in *Advanced Research on Electronic Commerce, Web Application, and Communication, Pt 2*, vol. 144, G. Shen and X. Huang, Eds. (Communications in Computer and Information Science, 2011, pp. 443-449.

[9] T. W. Jones, D., "Self-healing Autonomous Sensor Network (SASNet) Radiological/Nuclear (RN) prototype Printed Circuit Board (PCB) testing," Defence Research and Development Canada (DRDC) September 2017.

[10] F. Li, Y. Han, and C. Jin, "Practical access control for sensor networks in the context of the Internet of Things," *Computer Communications*, vol. 89–90, pp. 154-164, 9/1/ 2016.

[11] L. Li, "Localization in Self-Heating Autonomous Sensor Networks (SASNet): Studies on Cooperative Localization of Sensor Nodes Using Distributed Maps," Defence Research and Development Canada (DRDC) 01 Jan 2008.

[12] O. R. Merad Boudia, S. M. Senouci, and M. Feham, "A novel secure aggregation scheme for wireless sensor networks using stateful public key cryptography," *Ad Hoc Networks*, vol. 32, pp. 98-113, 9// 2015.

[13] J. A. Stankovic, "Adaptive and Reactive Security for Wireless Sensor Networks," Non Paid ADAS2007, Available: http://search.ebscohost.com/login.aspx?direct=true&db=nts&AN=ADP023722%2fXAB&site=ehost-live.

[14] D. Waller, "A Simulation Study of the Effectiveness of the Self-healing Autonomous Sensor Network for Early Warning Detection," Defence Research and Development Canada (DRDC)July 2009, Available: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc87/p531821.pdf.

[15] D. Waller, I. Chapman, and M. Michaud-Shields, "Concept of Operations for the Self-healing Autonomous Sensor Network," Defence R&D Canada - Centre for Operational Research and Analysis, Ottawa ON (CAN), DRDKIM 2, Defence R&D Canada, National Defence Headquarters, Ottawa, Canada K1A 0K2, Technical Memorandum DRDC-CORA-TM-2008-052, 01 Jul 2009 2009, Available: http://candid.drdc-rddc.gc.ca/cowdocs/cow1_e.html.

[16] S. Zhu, G. Cao, and P. Liu, "Distributed Self-healing Mechanisms for Securing Sensor Networks," Non Paid ADAS2010, Available: http://search.ebscohost.com/login.aspx?direct=true&db=nts&AN=ADA518946%2fXAB&site=ehost-live.

[17] A. Ponsford, R. McKerracher, Z. Ding, P. Moo, and D. Yee, "Towards a Cognitive Radar: Canada's Third-Generation High Frequency Surface Wave Radar (HFSWR) for Surveillance of the 200 Nautical Mile Exclusive Economic Zone," *Sensors,* vol. 17, no. 7, Jul 2017.

[18] S.-W. K. Jeemin Kim, Han Cha, Seunghwan Kim, Seong-Lyun Kim, "Sense-and-Predict: Harnessing Spatial Interference Correlation for Opportunistic Access in Cognitive Radio Networks," *Information Theory (cs.IT); Networking and Internet Architecture (cs.NI)* no. 1, p. 30, 4 Feb 2018. Accessed on: 25 July 2018 Available: https://arxiv.org/pdf/1802.01088.pdf

[19] J. M. Fuster, "The cognit: a network model of cortical representation," *International Journal of Psychophysiology,* vol. 60, no. 2, pp. 125-132, 2006.

[20] S. Haykin, Y. B. Xue, and P. Setoodeh, "Cognitive Radar: Step Toward Bridging the Gap Between Neuroscience and Engineering," *Proceedings of the IEEE,* vol. 100, no. 11, pp. 3102-3130, Nov 2012.

[21] S. Haykin, *Cognitive Dynamic Systems: Perception-Action Cycle, Radar, and Radio*. Cambridge University Press, 2012, p. 322.

[22] P. Labbé, "Could early adoption of internetworking of intelligent things provide significant advantages?," in *22nd International Command and Control Research and Technology Symposium (22nd ICCRTS)*, Los Angeles at the Army Research Laboratory - West and USC Institute for Creative Technologies, 2017, vol. Topic 3: Implications of the Internet of Intelligent Things, p. 22: ICCRTS, International Command and Control Institute.

[23] D. S. Alberts, *The Agility Advantage* (US DOD Command & Control Research Program). 2011.

[24] B. W. Young, "Future Integrated Fire Control: Integrated Fire Control for Future Aerospace Warfare," in *10th International Command and Control Research and Technology Symposium (10th ICCRTS): The future of command and control*, McLean, VA., 2005: Command and Control Research Program (U.S.)

[25] P. J. Walsh, "Development of a Physics-Aware Dead Reckoning Mechanism for Distributed Interactive Applications," Masters of Engineering Science by Research, National University of Ireland, Maynooth, 2011.

[26] J. Chudzikiewicz, J. Furtak, and Z. Zielinski, "Fault-tolerant techniques for the Internet of Military Things," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Milan, Italy, 2015, pp. 496-501: IEEE.

[27] J. Chudzikiewicz, J. Furtak, and Z. Zielinski, "Secure protocol for wireless communication within Internet of Military Things," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, 2015, pp. 508-513: IEEE.

[28] T. Kaur and D. Kumar, "Wireless multifunctional robot for military applications," in *2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS)*, 2015, pp. 1-5.

[29] J. Lee, L. Kant, A. McAuley, K. Sinkar, C. Graff, and M. Patel, "Planning & design of routing architectures for multi-tier military networks," in *MILCOM 2012 - 2012 IEEE Military Communications Conference*, 2012, pp. 1-7.

[30] NATO, "Advanced Autonomous Formation Control and Trajectory Management Techniques for Multiple Micro UAV Applications / Contrôle d'une formation autonome évoluée et gestion des trajectoires techniques d'applications pour micro UAV multiple," in "RTO-EN-SCI-195," Research and Technology Organization, Neuilly-sur-Seine (France) Systems Concepts and Integration Panel, Educational Notes RTO-EN-SCI-195, 01 Jun 2008, Available: http://candid.drdc-rddc.gc.ca/cowdocs/cow1_e.html.

[31] Missouri S&T, "Missouri S&T gets funding to develop battlefield 'smart dust'," *American Ceramic Society Bulletin,* Article vol. 89, no. 8, pp. 4-4, 2010.

[32] L. Kant, W. Chen, C. Lee, A. Sethi, and M. Natu, "D-FLASH: Dynamic Fault Localization and Self-Healing for Battlefield Networks," presented at the Proceedings for the Army Science Conference (24th), Orlando, Florida, 29 November - 2 December, 2005. Available: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA432120

[33] A. Kott, A. Swami, and B. J. West, "The Internet of Battle Things," *Computer,* Article vol. 49, no. 12, pp. 70-75, 2016.

[34] M. Maher, "Joint Tactical Radio System: Tactical Network Planning and Management," in *MILCOM 2007 - IEEE Military Communications Conference*, 2007, pp. 1-7.

[35] P. P. Ray, "Towards an Internet of Things based architectural framework for defence," in *2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, 2015, pp. 411-416.

[36] S. Ray, "In-Theatre Sense & Respond Logistics In-Theatre S&RL - TA5. Investigation of Selected Decision Support and Disruptive Technologies," Defence Research and Development Canada, Valcartier Research Centre, Quebec QC (CAN);Thales Canada, Quebec Que (CAN), Canada, Contract Report DRDC-RDDC-2016-C250, 01 Feb 2016, Available: http://candid.drdc-rddc.gc.ca/cowdocs/cow1_e.html.

[37] N. Suri *et al.*, "Analyzing the Applicability of Internet of Things to the Battlefield Environment," in *2016 International Conference on Military Communications and Information Systems (ICMCIS)*, Brussels, Belgium, 2016, pp. 117-122.

[38] Y. Chen and H. Hu, "Internet of intelligent things and robot as a service," *Simulation Modelling Practice and Theory,* vol. 34, pp. 159-171, 2013.

[39] J. Kaivo-oja, P. Virtanen, H. Jalonen, and J. Stenvall, "The effects of the internet of Things and big data to organizations and their knowledge management practices," in *International Conference on Knowledge Management in Organizations*, 2015, pp. 495-513: Springer.

[40] A. Arsénio, H. Serra, R. Francisco, F. Nabais, J. Andrade, and E. Serrano, "Internet of intelligent things: Bringing artificial intelligence into things and communication networks," in *Inter-cooperative Collective Intelligence: Techniques and Applications*: Springer, 2014, pp. 1-37.

[41] M. Kranz, P. Holleis, and A. Schmidt, "Embedded interaction: Interacting with the internet of things," *IEEE internet computing,* vol. 14, no. 2, pp. 46-53, 2010.

[42] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics,* vol. 10, no. 4, pp. 2233-2243, 2014.

[43] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," *Computer,* vol. 44, no. 9, pp. 51-58, 2011.

[44] W. Yeager and J.-H. Morin, "Introduction to Cloud and the Internet of Things: Challenges and Opportunities Minitrack," in *Proceedings of the 50th Hawaii International Conference on System Sciences / Cloud and Internet of Things:: Challenges and Opportunities Minitrack*, 2017, p. 5931.

[45] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internet of things (IIoT)–enabled framework for health monitoring," *Computer Networks,* vol. 101, pp. 192-202, 2016.

[46] C. Johnson, "Securing the Participation of Safety-Critical SCADA Systems in the Industrial Internet of Things," Accessed on: 24 April 2017, Available: http://eprints.gla.ac.uk/130828/1/130828.pdf

[47] M. R. Palattella *et al.*, "Internet of things in the 5G era: Enablers, architecture, and business models," *IEEE Journal on Selected Areas in Communications,* vol. 34, no. 3, pp. 510-527, 2016.

[48] P. Fraga-Lamas, T. M. Fernández-Caramés, M. Suárez-Albela, L. Castedo, and M. González-López, "A Review on Internet of Things for Defense and Public Safety," *Sensors*, Article vol. 16, no. 10, pp. 1-44, 2016.

[49] P. Stone *et al.*, "Artificial Intelligence and Life in 2030," *One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel*, 2016.

[50] A. Esteva *et al.*, "Dermatologist-level classification of skin cancer with deep neural networks," *Nature*, vol. 542, no. 7639, pp. 115-118, 2017.

[51] L. Kumar and A. Sureka, "Using Structured Text Source Code Metrics and Artificial Neural Networks to Predict Change Proneness at Code Tab and Program Organization Level," in *Proceedings of the 10th Innovations in Software Engineering Conference*, 2017, pp. 172-180: ACM.

[52] D. Jeannerat, "Human-and computer-accessible 2D correlation data for a more reliable structure determination of organic compounds. Future roles of researchers, software developers, spectrometer managers, journal editors, reviewers, publisher and database managers toward artificial-intelligence analysis of NMR spectra," *Magnetic Resonance in Chemistry*, vol. 55, no. 1, pp. 7-14, 2017.

[53] J. Lemley, S. Bazrafkan, and P. Corcoran, "Deep Learning for Consumer Devices and Services: Pushing the limits for machine learning, artificial intelligence, and computer vision," *IEEE Consumer Electronics Magazine*, vol. 6, no. 2, pp. 48-56, 2017.

[54] M. A. Zidan *et al.*, "A general memristor-based partial differential equation solver," *Nature Electronics*, vol. 1, no. 7, pp. 411-420, 2018/07/01 2018.

[55] K. Bourzac, "To Get AI in Everyday Gadgets, Engineers Go to Specialized Hardware," no. February, 14 Feb 2017 | 15:00 GMT. Accessed on: 14 June 2017, Available: http://spectrum.ieee.org/tech-talk/semiconductors/processors/to-get-ai-in-everyday-gadgets-engineers-go-to-specialized-hardware

[56] M. Cummings, "Artificial intelligence and the future of warfare," Chatham House for the Royal Institute of International Affairs1784131989, January 2017, Available: https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf.

[57] P. du Plessis, "Electronic-Warfare Training Using Low-Cost Software-Defined Radio Platforms," in *Defense Operational Applications Symposium (SIGE), Sao Jose dos Campos, Brazil*, 2013, pp. 119-123.

[58] R. Qiu *et al.*, "A Unified Framework for Cognitive Radio, Cognitive Radar, and Electronic Warfare—Tutorial, Theory, and Multi-GHz Wideband Testbed," *Sensors*, vol. 9, no. 8, p. 6530, 2009.

[59] Q. Xiao, "Cognitive Electronic Warfare: Evolution from Adaptive to Cognitive Technology," Defence Research and Development Canada (DRDC) November 2017.

[60] Q. Xiao, "A Conceptual Architecture of Cognitive Electronic Warfare System," in *COGNITIVE 2018 : The Tenth International Conference on Advanced Cognitive Technologies and Applications*, Barcelona, Spain, 2018, p. 5: International Academy, Research, and Industry Association (IARIA).

[61] P. Labbé, "DND/CAF Energy Horizons from Historical Data to the Potential Exploitation of Emerging Technologies," in *7th International Conference on Modelling and Simulation in Nuclear Science and Engineering (7ICMSNSE)*, Ottawa Marriott Hotel, Ottawa, Ontario, Canada, 2015, p. 18: Canadian Nuclear Society (CNS). Available: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc207/p802902_A1b.pdf.

[62] J. Fortin, D. Pudo, F. Théberge, and J.-F. Daigle, "Directed Energy Weapons; Impact Assessment of Emerging Disruptive Technologies (EDT)," ed: DRDC, 2015, p. 20.
[63] F. Peterkin and R. L. Gardner, "System Design and Assessment Notes, Note 42, High Power Microwave Applications," Directed Energy Warfare Office, Naval Surface Warfare CenterSeptember 2014, Available: http://ece-research.unm.edu/summa/notes/SDAN/0042.pdf, Accessed on: 9 April 2015.
[64] L. Palíšek, "Directed Energy Weapons in Modern Battlefield," *Advances in Military Technology (AiMT)*, vol. 4, no. 2, p. 12, December 2009 2009.
[65] Y.-D. Yao. (2014, 9 April 2015). *Introducion to Directed Energy* [Presentation]. Available: http://aoc-gardenstate.org/archive/AOC-DE-Seminar-10-15-2014.pdf
[66] J. P. M. Lichtman, S. Amuru, C. Shahriar, T. C. Clancy, R. M. Buehrer, J. H. Reed, "A Communications Jamming Taxonomy," *IEEE Security & Privacy*, Feb. 2016.
[67] M. Möstl, J. Schlatow, R. Ernst, H. Hoffmann, A. Merchant, and A. Shraer, "Self-aware systems for the Internet-of-Things," in *2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS)*, 2016, pp. 1-9: IEEE.
[68] S. Kounev *et al.*, "The Notion of Self-aware Computing," in *Self-Aware Computing Systems*: Springer, 2017, pp. 3-16.
[69] A. F. Cattoni, M. Musso, and C. S. Regazzoni, "Integration Between Navigation and Data-Transmission Systems in a Software Defined Radio Framework," 2007.
[70] A. F. Cattoni, M. Musso, and C. S. Regazzoni, "SDR Analog Front-End Architecture For Simultaneous Digitalization of Data Transmission and Navigation Signals," in *SDR Forum Technical Conference*, 2007.
[71] P. Labbé, D. Arden, L. Li, and Y. Ge, "Self-Aware / Situation Aware; Integrated Handhelds for Dispersed Civil and Military Urban Operations," *Inside GNSS*, vol. 2, no. 2, pp. 34-45, March/April 2007.
[72] P. Labbé, "GPS and GIS Integration in Mobile Equipment for Improved Mobile Emergency Operations," in *Proceedings of the 12th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 1999)*, Nashville, TN, 1999, pp. 545-554.
[73] P. Labbé, D. Arden, and L. Li, "GPS-INS-Radio and GIS Integration into Handheld Computers for Disperse Civilian and Military Urban Operations," in *Proceedings of the 2007 National Technical Meeting of The Institute of Navigation*, The Catamaran Resort Hotel, San Diego, CA, 2007, pp. 998 - 1010.
[74] J. A. Stankovic, "Robust and Secure Localization," Virginia Univ, Charlottesville 2009.
[75] S. Zhu, G. Cao, and P. Liu, "Distributed Self-healing Mechanisms for Securing Sensor Networks," State Univ. of New York at Buffalo, Amherst Research Foundation 2010.
[76] Y. Zhou, J. Schembri, L. Lamont, and J. Bird, "Experiments and analysis of stand-alone GPS for relative location discovery for SASNet," Defence R&D Canada, Ottawa ONT (CAN), Technical Memorandum DRDC-OTTAWA-TM-2010-140, 01 Aug 2010, Available: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc107/p533710_A1b.pdf.
[77] B. Ricard, "Le noeud de capteur SASNet," Defence Research and Development Canada, Valcartier Research Centre, Quebec QC (CAN), Canada, Scientific Report DRDC-RDDC-2014-R70, 01 Dec 2014, Available: http://candid.drdc-rddc.gc.ca/cowdocs/cow1_e.html.
[78] L. Li, "Localization in Self-Healing Autonomous Sensor Networks (SASNet): Studies on Cooperative Localization of Sensor Nodes Using Distributed Maps," Defence R&D Canada - Ottawa, Ottawa ONT (CAN), Ottawa, Canada, Technical Report DRDC-OTTAWA-TR-2008-020, 01 Jan 2008, Available: http://candid.drdc-rddc.gc.ca/cowdocs/cow1_e.html.

[79] M. Deziel, "A Reliable Transport Protocol for Resource Constrained Nodes / Un Protocole de transport avec garantie de livraison pour les appareils de communications aux ressources limitées," Defence Research and Development Canada, Ottawa Research Centre, Ottawa ON (CAN);Communications Research Centre, Ottawa ONT (CAN), Contract Report DRDC-RDDC-2014-C109, 01 Jun 2014, Available: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc198/p800537_A1b.pdf.

[80] C. Widdis, "SASNet Sensor Signal Processing Algorithms: Part 1," Defence R&D Canada - Valcartier, Valcartier QUE (CAN);MacDonald Dettwiler and Associates Ltd, Dartmouth NS (CAN), Contractor Report DRDC-VALCARTIER-CR-2009-010, 01 Jan 2009.

[81] W. Shen, "Self-Reconfigurable Robots for Adaptive and Multifunctional Tasks," presented at the AIAA SPACE 2009 Conference & Exposition, AIAA SPACE Forum, Pasadena, California, 2008.

[82] D. Waller, "A Simulation Study of the Effectiveness of the Self-healing Autonomous Sensor Network for Early Warning Detection," Defence R&D Canada - Centre for Operational Research and Analysis, Ottawa ON (CAN), Technical Memorandum DRDC-CORA-TM-2009-019, 01 Jul 2009, Available: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc87/p531821.pdf.

[83] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, 2015.

[84] C. Kolias, A. Stavrou, J. Voas, I. Bojanova, and R. Kuhn, "Learning Internet-of-Things Security" Hands-On"," *IEEE Security & Privacy*, vol. 14, no. 1, pp. 37-46, 2016.

[85] H. Ning, H. Liu, and L. T. Yang, "Cyberentity Security in the Internet of Things," *Computer*, vol. 46, no. 4, pp. 46-53, 2013.

[86] Y. Deng, L. Wang, K.-K. Wong, A. Nallanathan, M. Elkashlan, and S. Lambotharan, "Safeguarding massive MIMO aided hetnets using physical layer security," in *2015 International Conference on Wireless Communications & Signal Processing (WCSP)*, 2015, pp. 1-5: IEEE.

[87] F. Delaveau, A. Evesti, J. Suomalainen, and N. Shapira, "Active and passive eavesdropper threats within public and private civilian wireless-networks–existing and potential future countermeasures–a brief overview," *Proceedings of SDR*, pp. 11-20, 2013.

[88] P. Pirinen, "A brief overview of 5G research activities," in *2014 1st International Conference on 5G for Ubiquitous Connectivity (5GU)*, 2014, pp. 17-22: IEEE.

[89] G. Ding, Q. Wu, L. Zhang, Y. Lin, T. A. Tsiftsis, and Y.-D. Yao, "An amateur drone surveillance system based on the cognitive Internet of Things," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 29-35, 2018.

[90] P. Labbé, "Would next-generation of cognitive radar (CR) technologies provide significant advantage? (Document in the publication process)," ed. Ottawa, Canada: Defence Research and Development Canada (DRDC), 2018, p. 32.

[91] T. S. K Krishnan, S Sarraf, "Cognitive Dynamic Systems: A Technical Review of Cognitive Radar," 2016.

[92] S. Haykin, "Radar vision," in *Record of the IEEE 1990 International Radar Conference*, Arlington, VA, USA, 1990, pp. 585-588: IEEE.

[93] S. Haykin, "Adaptive radar: Evolution to cognitive radar," in *IEEE International Symposium on Phased Array Systems and Technology*, 2003, p. 613: IEEE.

[94] S. Haykin, "Cognitive Radar Networks," in *IEEE Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP), 2005: First International Workshop on Computational Advances in Multi-Sensor Adaptive Processing*, Puerto Vallarta, Mexico, 2005, pp. 1-3: IEEE.

[95] S. Haykin, "Cognitive radar - A way of the future," *IEEE Signal Processing Magazine,* vol. 23, no. 1, pp. 30-40, Jan 2006.
[96] S. Haykin, "Cognitive radar networks," in *Fourth IEEE Workshop on Sensor Array and Multichannel Processing,* 2006, pp. 1-24: IEEE.
[97] S. Haykin, "Cognitive Dynamic Systems: Radar, Control, and Radio," *Proceedings of the IEEE,* vol. 100, no. 7, pp. 2095-2103, Jul 2012.
[98] S. Haykin, "Cognitive Networks: Radar, Radio, and Control for New Generation of Engineered Complex Networks," in *2013 IEEE Radar Conference (Radar),* Ottawa, ON, Canada, 2013: IEEE.
[99] S. Haykin and J. M. Fuster, "On cognitive dynamic systems: Cognitive neuroscience and engineering learning from each other," *Proceedings of the IEEE,* vol. 102, no. 4, pp. 608-628, 2014.
[100] S. Haykin, Y. B. Xue, and T. N. Davidson, "Optimal waveform design for cognitive radar," in *2008 42nd Asilomar Conference on Signals, Systems and Computers,* Pacific Grove, CA, USA, 2008, vol. 1-4, pp. 3-7: IEEE.
[101] S. Haykin, A. Zia, I. Arasaratnam, and Y. B. Xue, "Cognitive Tracking Radar," in *2010 IEEE Radar Conference,* Washington, DC, USA, 2010, pp. 1467-1470.
[102] S. Haykin, A. Zia, Y. Xue, and I. Arasaratnam, "Control theoretic approach to tracking radar: First step towards cognition," *Digital Signal Processing,* vol. 21, no. 5, pp. 576-585, 2011.
[103] W. Au and S. Martin, "Why dolphin biosonar performs so well in spite of mediocre 'equipment'," *The Institution of Engineering and Technology (IET) Radar, Sonar & Navigation,* vol. 6, no. 6, pp. 566-575, 2012.
[104] T. Kaak and G. Schmidt, "An Introduction to Real-time Cognitive SONAR Systems Utilizing Novel MIMO Approaches," in *Deutsche Gesellschaft für Akustik (DEGA),* Kiel, Germany, 2017.
[105] N. Sharaga, J. Tabrikian, and H. Messer, "Optimal Cognitive Beamforming for Target Tracking in MIMO Radar/Sonar," *IEEE Journal of Selected Topics in Signal Processing,* vol. 9, no. 8, pp. 1440-1450, Dec 2015.
[106] L. Xiaohua, L. Yaan, L. Guancheng, and Y. Jing, "Research of the principle of cognitive sonar and beamforming simulation analysis," in *2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC),* 2011, pp. 1-5.
[107] F. Castaño, G. Beruvides, R. E. Haber, and A. Artuñedo, "Obstacle Recognition Based on Machine Learning for On-Chip LiDAR Sensors in a Cyber-Physical System," *Sensors,* vol. 17, 2017.
[108] A. Rajagopal, K. Chellappan, S. Chandrasekaran, and A. P. Brown, "A machine learning pipeline for automated registration and classification of 3D lidar data," in *Geospatial Informatics, Fusion, and Motion Video Analytics VII,* Anaheim, California, 2017, vol. 10199, p. 101990D: International Society for Optics and Photonics.
[109] D. Steinhauser, O. Ruepp, and D. Burschka, "Motion segmentation and scene classification from 3D LIDAR data," in *Intelligent Vehicles Symposium, 2008 IEEE,* Eindhoven, Netherlands, 2008, pp. 398-403: IEEE.
[110] H. M. Roff and D. Danks, "'Trust but Verify': The difficulty of trusting autonomous weapons systems," *Journal of Military Ethics,* pp. 1-19, 2018.
[111] K. Siau and W. Wang, "Building Trust in Artificial Intelligence, Machine Learning, and Robotics," *Cutter Business Technology Journal,* vol. 31, no. 2, pp. 47-53, 2018.