AI and IoT Mapping and the Transition to an Interconnected Cyber Defence and Intelligence Capabilities

Joseph JONES[1], Angela IONIȚĂ, PhD[2], Ioan-Cosmin MIHAI, PhD[3]
[1] OS2INT, Skive, Denmark
joseph.jones@os2int.com
[2] Romanian Academy
aionita@racai.ro
[3] Police Academy, Romania
cosmin.mihai@academiadepolitie.ro

Abstract

This paper brings together authors from a diverse range of technical areas to discuss the evolving cyber threat landscape and how military forces, have transformed their capabilities to meet present-day operational challenges in cyberspace. The Internet of Things (IoT) is based on the premise that enough data can lead to new perspectives on processes and systems. With over 7 billion IoT devices connected today, experts expect that number to increase to 22 billion by 2025. They can be used to support decisions and new products and services, or they can lead to internal savings and new external revenue streams. Despite countless discussions and opinions on the definition of AI in its various facets, successful IoT implementation projects require major actors to play their part, but in conjunction with human experts to work with to make better decisions in cyberspace, improving the quality of human-machine team's actions in asymmetric operations. The Defence domain already looking at ways to organize better human-machine teams, which promise to boost individual and team performance, reduce threats to humans, enable new operating concepts, and ultimately boost national power.

Index terms: AI, Decision-making, Human-machine teams, Hyperautomation, IoT

1. Introduction

In the digital age we are going through, we must be aware that the Internet of Things (IoT) is driving significant and impactful change across verticals markets. While IoT devices can be found throughout our homes, the number of IoT devices that are being deployed across industrial environments and defense is also growing simultaneously.

Each application is unique and may require different forms of IoT connectivity and it is important for organizations to understand and weigh the pros and cons of each technology before deploying to ensure they are receiving proper connectivity. IoT has become essential to create efficiencies and improve lives globally, and with this comes the need for organizations to pivot and adapt to technological advances to stay relevant, competitive, and effective.

According to [30] it is expected that by 2026, the global IoT market will reach a value of $1.4 billion. This growing adoption is said to be "*fueling the next industrial revolution of connectivity*," shifting the way industries and organizations approach processes and systems with efficiencies and downtime top of mind.

"As IoT technology continues to evolve, businesses and organizations are progressing with it, taking advantage of the opportunity to develop more efficient and effective processes. While the "industrial revolution of connectivity" may be a work in progress, IoT technologies will continue to drive progress and change everywhere." [30].

The most recognizable shift in the modern-day battlefield is that information became the most effective weapon of all and moving towards an interconnected cyber defence and intelligence capabilities. The situational awareness based on the collected information became the core of every operation. Information operations as a new domain entered the battlefield, the integrated network of sensors, weapon systems and platforms became force multiplier [6].

According to Statista [23], "*The total installed base of Internet of Things (IoT) connected devices is projected to amount to 75.44 billion worldwide by 2025, a fivefold increase in ten years*." (Fig. 1).

In the future, it is expected that operations will rely less on human soldiers and more on interconnected technology, leveraging advancements in embedded systems and machine intelligence to achieve superior defense capabilities. In the future of new concepts, new technologies, new tools, and processes appeared based on the concept of network-centric warfare.

Over time, several different terms have been introduced to describe the use of IoT technology for reconnaissance, environment surveillance, unmanned warfare, and other combat purposes. These terms include the Internet of Military Things (IoMT) [7], the Internet of Battle Things [20], and the Internet of Battlefield Things (IoBT).

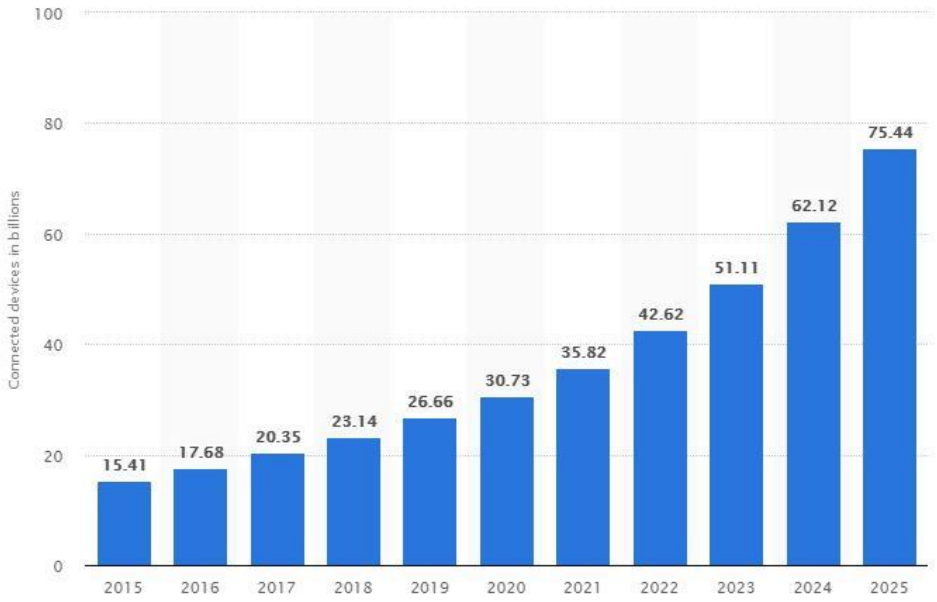


Fig. 1. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025

One of the best visions of the future was made by Defense Secretary of USA, Lloyd Austin [22]: "*What we need is the right mix of technology, operational concepts and capabilities -- all woven together in a networked way that is so credible, flexible and formidable that it will give any adversary pause*" Austin said. "*We need to create advantages for us and dilemmas for them."*

2. Operational and intelligence decision-making in the evolution of Remote and Automated Systems (RAS)

Digital technologies lie at the heart of nearly every domain today. The automation and greater connectedness they afford have revolutionized the world's institutions - but they have also brought

risk e. g. in the form of cyberattacks. Threat intelligence is knowledge that allows you to prevent or mitigate those attacks. Rooted in data, threat intelligence provides context - like who is attacking, what their motivation and capabilities are, and what indicators of compromise in some systems to look for - that helps make informed decisions about security. "*Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and action-oriented advice about an existing or emerging menace or hazard to assets. This intelligence can be used to inform decisions regarding the subject's response to that menace or hazard.*" [26].

For the image to be as close as possible to the real one, it is necessary firstly, for this section, to highlight what automation and automated system refers to.

Automation is making waves in many industries worldwide and encompasses a wide range of technologies including endpoint management, robotic process automation (RPA), artificial intelligence (AI) and machine learning (ML).

Without any doubts, the trends highlighted in Gartner's top ten strategic technology for 2021 [37] have an impact on all areas of life and goes beyond the automation provided by rigid programming models, and they exploit AI to deliver advanced behaviors that interact more naturally with their surroundings and with people. As predicted by Gartner, as the technology capability improves, regulation permits and social acceptance grows, autonomous things will increasingly be deployed in uncontrolled public spaces.

For a better understanding of the evolution and new trends, it would be good to go through a short history of autonomous military systems offered by literature. This short history tells us that autonomous military systems have been used by armed forces around the world for many decades. All of these can trace their past to as early as the First World War and their importance to the battlefields of the future is expected to grow exponentially.

Today they can be found performing various combat roles from search and rescue, explosive disarmament, fire support, reconnaissance, logistics support and, of course, lethal combat duties to name but a few. Many believe will see fully automated lethal autonomous systems soon potentially making the role of human soldier obsolete.

Despite other fears, it should be noted that many military vehicles with combat capability are prevented from being fully autonomous presently. This is by design to ensure there is some human input at times to ensure targets are not within restricted fire zones under the laws of war set out in the Geneva Convention [8].

In [25] there is a quick tour of the history of autonomous military systems (including remote controlled, semi- and fully-autonomous) and highlighted some interesting examples. But there is an enormous variety of autonomous military systems and, as such, it has not been possible to cover them all. Autonomous systems for the military, also called autonomous robots or remote-controlled drones, have had a surprisingly long and interesting history. Though they have come to prominence and large-scale use in recent years, their ancestors were first used during the First and Second World War and the Cold War that followed them.

Military autonomous systems are likely to grow in numbers and roles exponentially in the future as armies continue to develop and invest in this technology. Some military experts believe that not only will combat robots be a reality very soon but also that robots will outnumber actual service personnel in the U.S. Army by 2025.

Automation was highlighted in Gartner's published top ten strategic technology trends for 2020 [38]. One trend is what Gartner calls "*hyperautomation*" the combination of multiple machine learning, packaged software, and automation tools to deliver work, referring to all the steps of automation-discover, analyze, design, automate, measure, monitor and reassess. Understanding the range of automation mechanisms, how they relate to one another and how they can be combined and coordinated is a major focus for hyperautomation.

Another trend identified by Gartner is "*autonomous things."* [39]. These are physical devices that use AI to automate functions previously performed by humans. The most recognizable forms of autonomous things are robots, drones, autonomous vehicles/ships, and appliances. The main purpose of an automated system is to help speed up a process. Automated systems eliminate the need for human interference to complete a task. Tasks that are time-consuming or inconvenient are often incorporated into systems.

Automated Systems have key components that allow them to function properly including a control system, a way to interpret and distribute data and a human interface. Programmable logic allows the system to process data and control it. Automated systems have been incorporated into production lines and machines for years. Several industrial domains use automated systems to increase production and reduce costs. An example is the computer industry where there are many tasks that do not require constant human attention. Software can be used to complete several different tasks and automatically post the results. Bots can be programmed to click objects on the screen, send messages at preset times or interact on social networks using artificial intelligence. Another common example is an ATM, which can process banking transactions without a teller.

According to Kaseya [40] in different stages of their evolution automation technologies refers to a simple three-level hierarchy presented in Fig. 3.

Another trend identified by Gartner refer to *multiexperience.* Through 2028, the user experience will undergo a significant shift in how users perceive the digital world and how they interact with it. Conversational platforms are changing the way in which people interact with the digital world. Virtual reality (VR), augmented reality (AR) and mixed reality (MR) are changing the way in which people perceive the digital world. This combined shift in both perception and interaction models leads to the future multisensory and multimodal experience.

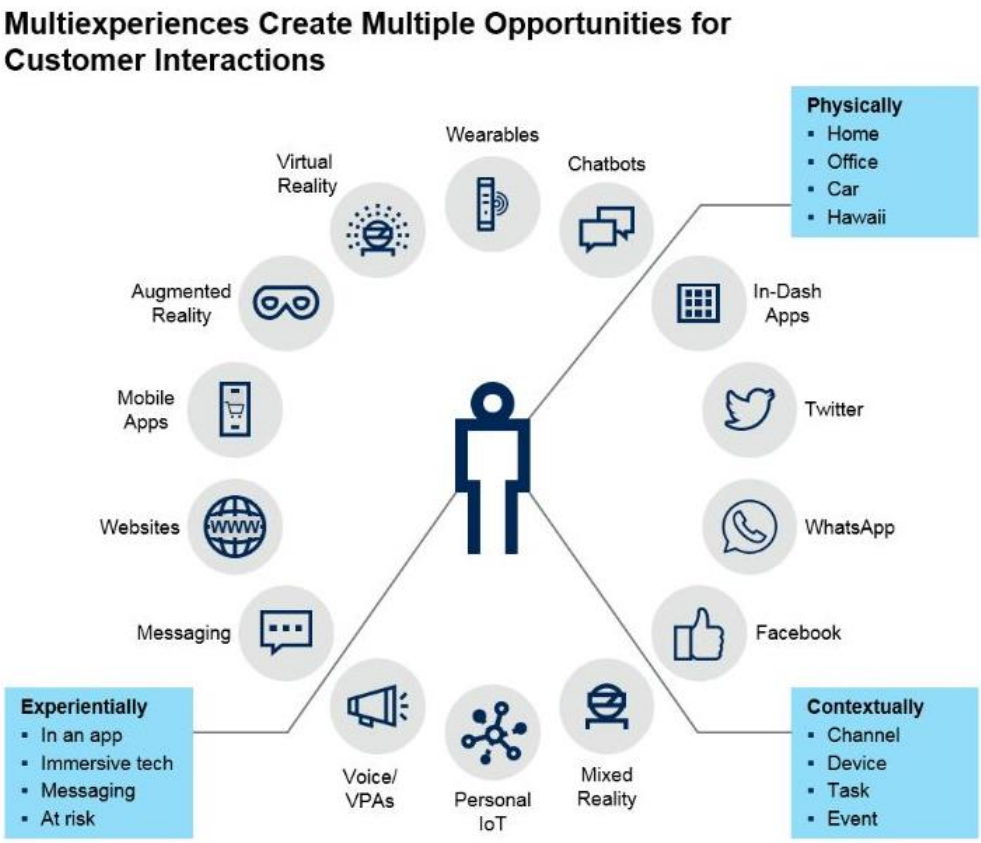


Fig. 2. Opportunities created by multiexperiences
Source: Gartner, 2020

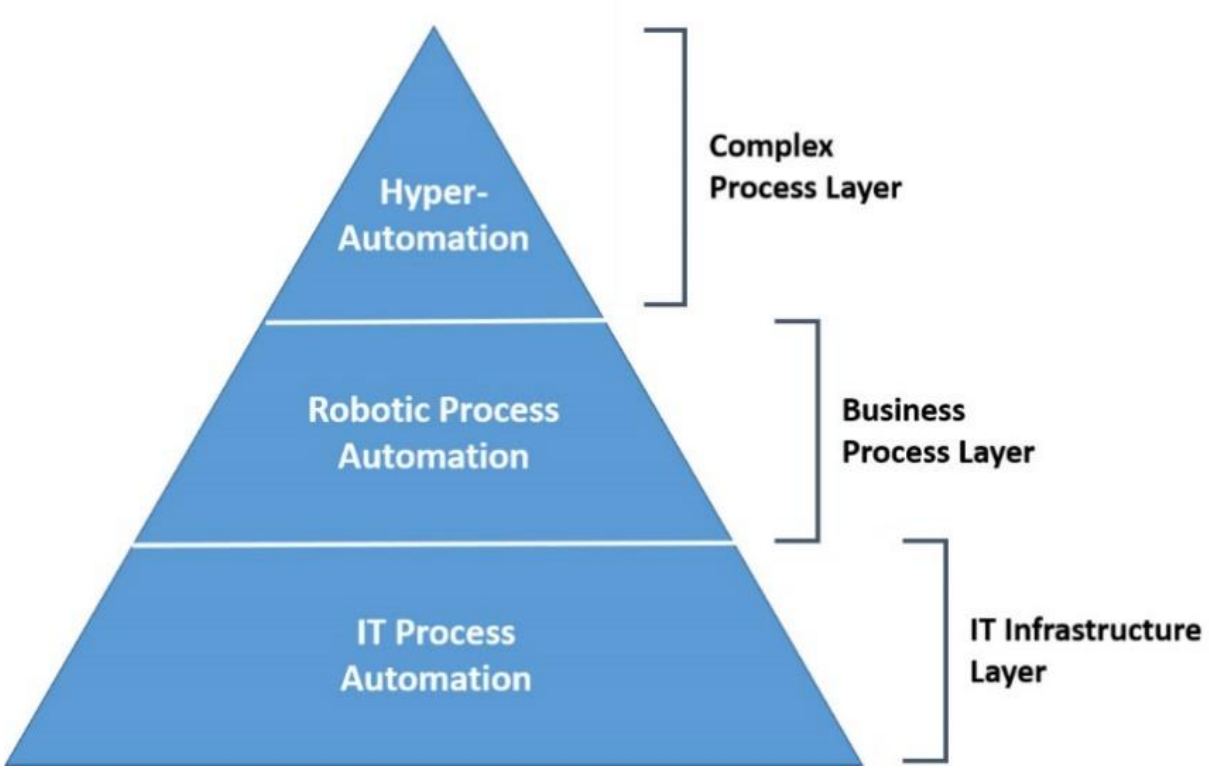
Through 2023, Gartner expects four key aspects of the *democratization* trend to accelerate, including democratization of data and analytics (tools targeting data scientists expanding to target the professional developer community), democratization of development (AI tools to leverage in custom-developed applications), democratization of design (expanding on the low-code, no-code phenomena with automation of additional application development functions to empower the citizen-developer) and democratization of knowledge (non-IT professionals gaining access to tools and expert systems that empower them to exploit and apply specialized skills beyond their own expertise and training).
Democratization is focused on providing people with access to technical expertise (e.g., ML, application development) or business domain expertise (for example, sales process, economic analysis) via a radically simplified experience and without requiring extensive and costly training. "Citizen access" (e.g., citizen data scientists, citizen integrators), as well as the evolution of citizen development and no-code models, are examples of democratization.

Over the next 10 years increasing levels of physical and cognitive *human augmentation* will become prevalent as individuals seek personal enhancements. This will create a new "consumerization" effect where employees seek to exploit their personal enhancements - and even extend them - to improve their office environment.

Human augmentation explores how technology can be used to deliver cognitive and physical improvements as an integral part of the human experience.

Another trend focused on *transparency* and *traceability* and refer to a range of attitudes, actions and supporting technologies and practices designed to address regulatory requirements, preserve an ethical approach to use of AI and other advanced technologies, and repair the growing lack of trust in companies. As organizations build out transparency and trust practices, they must focus on three areas:

(1) AI and ML;
(2) personal data privacy, ownership, and control; and
(3) ethically aligned design.



IT Process Automation	Robotic Process Automation	Hyperautomation
The foundational layer of all automation technologies is the automation of IT processes. This involves the automation of routine IT tasks and workflows (e.g., server maintenance, software patch management and software updates and includes auto-remediation of IT incidents and associated service tickets).	RPA is the business process layer. In RPA, simple, repeatable rules are followed by "bots" or virtual systems to automate manual computing steps or simple business processes. Research firm Gartner predicted that the global robotic process automation (RPA) market revenue will reach $1.89 billion in 2021 - an increase of 19.5 percent from 2020.	Hyperautomation brings together artificial intelligence/machine learning (AI/ML) tools with RPA to enable the automation of complex business processes. Hyperautomation can lead to real digital transformation of the business. As one of the top 10 strategic trends of 2021 touted by Gartner (https://youtu.be/s3rlYW cwdDY), the idea of hyperautomation is to automate "anything" that can be automated. Implementing hyperautomation requires streamlining entire processes, getting rid of legacy applications, and enforcing lean, optimized, and interconnected processes.
There are some benefits of IT Process Automation: reduced human error (Automating IT processes ensures there is accuracy in every step and reduces the chances of errors occurring), increased IT operational efficiency (IT process automation frees up IT technicians to work on more challenging tasks and strategic), higher system uptime (auto-remediation of incidents means that problems are resolved faster, and systems and services have higher availability).	Among benefits of RPA are cost-effectiveness, improved productivity and quality of work, better decision making. Challenges with RPA count: scalability (unless the appropriate implementation processes are chosen with RPA, scaling can become an issue) and enabling end-to-end automation (RPA tools may be insufficient for complex processes and in such cases, may break down these processes into simpler tasks that can be automated with RPA or progress to hyperautomation).	Among benefits of Hyperautomation are: End-to-end automation (starting from process discovery to measuring return-on-investment (ROI), all of this can potentially be automated), significant transformation (when every part of a complex process is automated, the whole operation can be transformed). There are some challenges with Hyperautomation. The major challenge with hyperautomation is automating complex processes. Grappling with process complexity can cause frustration and increase implementation costs

Fig. 3. Hierarchy of Automation Technologies (adopted from [10])

It is important to perceive that we cope with significant shift from the centralized model of most public cloud services and that will lead to a new era in cloud computing: the era of *distributed cloud* (the distribution of public cloud services to different locations while the originating public cloud provider assumes responsibility for the operation, governance, updates to and evolution of the services).

According Gartner [39], another area is represented by *practical Blockchain* which remains immature for enterprise deployments due to a range of technical issues including poor scalability and interoperability.

AI and ML will continue to be applied to augment human decision making across a broad set of use cases. While this creates great opportunities to enable hyperautomation and leverage autonomous things to deliver business transformation, it creates significant new challenges for the security team [41] and risk leaders with a massive increase in potential points of attack with IoT, cloud computing, microservices and highly connected systems in smart spaces. *Security and risk leaders* should focus on three key areas - protecting AI-powered systems, leveraging AI to enhance security defense, and anticipating nefarious use of AI by attackers.

On the second, it must clarify what is *Operational Intelligence* (OI) and how it works, and which are OI benefits and challenges. OI is an approach to data analysis that enables decisions and actions in different, including business, operations to be based on real-time data as it is generated or

collected. Typically, the data analysis process is automated, and the resulting information is integrated into operational systems for immediate use by specialists.

OI applications are primarily targeted at front-line workers who, hopefully, can make better-informed decisions or take faster action on issues if they have access to timely intelligence and analytics. In addition, OI can be used to automatically trigger responses to specified events or conditions.

What is now known as OI evolved from operational business intelligence, an initial step focused more on applying traditional Business Intelligence (BI) querying and reporting. OI takes the concept to a higher analytics level, but operational BI is sometimes still used interchangeably with operational intelligence as a term.

In most OI initiatives, data analysis is done in tandem with data processing or shortly thereafter, so workers can quickly identify and act on problems and opportunities in different operations. Deployments often include real-time intelligence systems set up to analyse incoming data, plus real-time data integration tools to pull together different sets of relevant data for analysis.

Today, the cybersecurity industry faces numerous challenges - increasingly persistent and devious threat actors, a daily flood of data full of extraneous information and false alarms across multiple, unconnected security systems, and a serious shortage of skilled professionals.

Some specialised people try to incorporate threat data feeds into their network, but do not know what to do with all that extra data, adding to the burden of analysts who may not have the tools to decide what to prioritize and what to ignore.

Everyone can benefit from threat intelligence. Cyber threat intelligence is widely imagined to be the domain of elite analysts. It adds value across security functions for organizations of all sizes.

When threat intelligence is treated as a separate function within a broader security paradigm rather than an essential component that augments every other function, the result is that many of the people who would benefit the most from threat intelligence do not have access to it when they need it.

Security operations teams often prove routinely unable to process the alerts they receive - threat intelligence integrates with the security solutions already use, helping automatically prioritize and filter alerts and other threats. Vulnerability management teams must more accurately prioritize the most important vulnerabilities with access to the external insights and context provided by threat intelligence. And risk analysis and other high-level security processes could be enriched by the understanding of the current threat landscape that threat intelligence provides, including key insights on threat actors, their tactics, techniques, and procedures, and more from data sources across the web.

A cyber threat intelligence solution can address each of these issues. The best solutions use ML to automate data collection and processing, integrate with existing solutions, take in unstructured data from disparate sources, and then connect the dots by providing context on indicators of compromise (IoCs) and the tactics, techniques, and procedures (TTPs) of threat actors.

Threat intelligence is actionable - it is timely, provides context, and can be understood by the people in charge of making decisions.

Stream processing systems and big data platforms can also be part of the OI picture, particularly in applications that involve large amounts of data and require advanced analytics capabilities. In addition, various Information Technology (IT) vendors have combined data streaming, real-time monitoring, and data analytics tools to create specialized operational intelligence platforms.

As data is analyzed, organizations often present operational metrics, key performance indicators (KPIs) and insights to the workers in interactive dashboards that are embedded in the systems they use as part of their jobs; data visualizations are usually included to help make the information easy to understand. Alerts can also be sent to notify users of developments and data points that require their attention, and automated processes can be kicked off if predefined thresholds or other metrics are exceeded.

Between the benefits of OI implementations there is the ability to address operational issues and opportunities as they arise -- or even before they do, as in the case of predictive maintenance. OI also empowers workers to make more informed -- and conceivably better -- decisions on a day-by-day basis. Ultimately, if managed successfully, the increased visibility and insight into operations can lead to higher revenue and competitive advantages over rivals.

But there are also challenges. Building operational intelligence architecture typically involves piecing together different technologies, and there are numerous data processing platforms and analytics tools to choose between, some of which may require new skills. High performance and sufficient scalability are also needed to handle the real-time workloads and large volumes of data common in OI applications without choking the system.

The *threat intelligence* belongs three dimensions (Fig. 4): **strategic** (broader trends typically meant for a non-technical audience), **tactical** (outlines of the tactics, techniques, and procedures of threat actors for a more technical audience), **operational** (technical details about specific attacks and campaigns).

Fig. 4. The three dimensions of threat intelligence (adopted from [42])

Strategic threat intelligence [43] provides a broad overview of an organization's threat landscape. It is intended to inform high-level decisions made by decision makers - as such, the content is generally less technical and is presented through reports or briefings. Good strategic intelligence should provide insight into areas like the risks associated with certain lines of action, broad patterns in threat actor tactics and targets, and geopolitical events and trends.

Policy documents from nation-states or nongovernmental organizations, news from local and national media, industry- and subject-specific publications, or other subject-matter experts, white papers, research reports, and other content produced by security organizations there are as many common sources as possible of information for strategic threat intelligence.

Producing strong strategic threat intelligence starts with asking focused, specific questions to set the intelligence requirements. It also takes analysts with expertise outside of typical cybersecurity skills - in particular, a strong understanding of socio-political and business concepts.

Although the final product is non-technical, producing effective strategic intelligence takes deep research through massive volumes of data, often across multiple languages. That can make the initial collection and processing of data too difficult to perform manually, even for those rarefied analysts who possess the right language skills, technical background, and tradecraft. A threat intelligence solution that automates data collection and processing helps reduce this burden and allows analysts who do not have as much expertise to work more effectively.

Tactical threat intelligence [44] outlines the tactics, techniques, and procedures (TTPs) of threat actors. It usually includes technical context and is used by personnel directly involved in the defence, such as system architects, administrators, and security staff.

Reports produced by security vendors are often the easiest way to get tactical threat intelligence. Look for information in reports about the attack vectors, tools, and infrastructure that attackers are using, including specifics about what vulnerabilities are being targeted and what exploits attackers are leveraging, as well as what strategies and tools that they may be using to avoid or delay detection.

Tactical threat intelligence should be used to inform improvements to existing security controls and processes and speed up incident response. Because many of the questions answered by tactical intelligence are unique and need to be answered on a short deadline - for example, "*Is this critical vulnerability being exploited by threat actors targeting my industry present in my systems?"* - having a threat intelligence solution that integrates data from within own network is crucial.

Operational intelligence [45] is knowledge about cyber-attacks, events, or campaigns. It gives specialized insights that help incident response teams understand the nature, intent, and timing of specific attacks.

Because this usually includes technical information - information like what attack vector is being used, what vulnerabilities are being exploited, or what command and control domains are being employed - this kind of intelligence is also referred to as technical threat intelligence. A common source of technical information is threat data feeds, which usually focus on a single type of indicator, like malware hashes or suspicious domains. But if technical threat intelligence is strictly thought of as deriving from technical information like threat data feeds, then technical and operational threat intelligence are not totally synonymous - more like a Venn diagram with huge overlaps. Other sources of information on specific attacks can come from closed sources like the interception of threat group communications, either through infiltration or breaking into those channels of communication.

Consequently, there are a few barriers to gathering this kind of intelligence: **access**, **noise**, **obfuscation.**

Threat intelligence solutions that rely on ML processes for automated data collection on a large scale can overcome many of these issues when trying to develop effective operational threat intelligence. A solution that uses natural language processing, for example, will be able to gather information from foreign-language sources without needing human expertise to decipher it.

Thirdly, in [9] it is argued that AI will change decision-making in the defence and security arena in four principal ways. First, by enabling 'cognitive manoeuvre' the use of predictive analytics to enable much earlier intervention. Second, by forcing humans to take themselves 'out of the loop' for decision-making by out-performing them in an increasing number of domains. Third, by providing advice that is correct, but difficult to explain. Fourth, in the short term, by driving unprecedented rigour into decision-making processes, forcing decision-makers to be much more explicit about the mental models on which they are basing decisions, to enable comparison with automated analytics.

3. AI-development and conflict

The global artificial intelligence market size is expected to reach $169,411.8 million in 2025, from $4,065.0 million in 2016 growing at a CAGR of 55.6% from 2018 to 2025. Artificial intelligence has been one of the fastest-growing technologies in recent years [45]. AI is being used in every industry and is projected to be a core skill for the future. Artificial Intelligence represents a huge opportunity across virtually every sector. It has already proven to be disruptive, but it is anticipated that it will be much more widespread over the next few years. The professionals differentiate between an objective nature and a subjective character of conflict. Nature of conflict describes what conflict is and character of conflict describes how it is fought. Nature of conflict may be violent, interactive between opposing wills and fundamentally political. Conflict's character is influenced by technology,

law, ethics, culture, methods of social, political, and military organization and other factors that change across time and place. Character of conflict changes as much as professionals organize themselves to fight conflicts.

It has been not appreciated the changes in how conflict was tackling or in the character of conflict. Future development and deployment of human-machine teams and autonomous weapons systems represents such a shift in the character of conflict.

In near future in autonomy and machine learning it is expected significant advance, to include the emergence of robots working together in groups and as swarms. New and powerful robotic systems will be used to perform complex actions, make autonomous decisions, provide intelligence, surveillance, and reconnaissance, coverage, and speed response times over wider areas of the globe. Professional organizations must plan now for this new era of conflicts. Governments must be prepared for the political, strategic, and ethical dimensions of this shift in the character of conflicts.

Major technological breakthroughs that could occur in robotics as well as information, cognitive, and material sciences are, by themselves, truly revolutionary. Applications of AI have the potential to change the very nature of conflicts. At the strategic level, this could affect e.g., how the armed forces organize ground forces, how it fights and what types of major weapon systems it will need. At the operational and tactical levels, enemy's AI capabilities could dictate specific weapon systems design, the development of new types of units to address his AI capabilities and how brigade to squad level units conduct tactical operations [36].

But some questions remain:

- should the technology develop the way it is expected to, removing a man from the loop could allow machine conflict to be fully unleashed?
- AI so radically changes everything so that war itself may not resemble what it has been for the entirety of human history?

From this point of view, at the present state of development AI technologies are considered immature. Modern unmanned aircraft in service can operate autonomously but cannot yet execute the sorts of complex missions that manned equivalents can achieve. Land robots are clumsy on uneven terrain. Concepts fail to deliver significant breakthroughs in autonomous decision making. There is considerable wariness that the hype and publicity surrounding deep learning will not pan out as dramatic breakthroughs.

The present developments of AI technologies in military domain have not reached the level when it can be said that it would change the nature of war. In fact, it is in a nascent state of development. However, the scenario is changing fast. Despite best efforts, no nation-state can ever be fully prepared for the character of the next war. As such, potential military applications of emergent technology should not be viewed as a panacea for the chaos, friction, and chance that will continue to define war in the future. Regardless of the possibilities offered by technological advances, success in the next conflict is likely to be just as reliant on human genius.

Today, we are at a major inflection point, one in which technology is reshaping the way conflicts are tackling [13]. "*The future of warfare will be shaped by the role of smaller drones; robots on the battlefield, offensive cyberwar capabilities, extraordinary surveillance capabilities both on the battlefield and of individuals, greater reliance on special operations forces operating in non-conventional conflicts and militarization of the space"*. [24].

There are arguments that AI has the potential to go beyond shaping the character of conflict and change the nature of conflict itself because conflicts it is expected to be fought by robotic systems, not people. AI has the potential to engage in planning and decision making that were previously human endeavours.

The character of conflicts changes together with the tools that become available and how they influence the ways professionals organize themselves to fight conflicts. AI is one of the major developments of our time. ML and particularly the implications that go with it, is shaking up many

aspects of how things do, allowing us to deploy AI software where previously used a human or a more inefficient process. Sometimes this is to the consternation of people, particularly those who worry about AI systems and machine intelligence taking over human jobs, or perhaps the sci-fi scenario of AI being intelligent and organized enough to overrule humans. AI systems have the potential to increase the speed with which countries can fight. Even if humans are still making final decisions about the use of lethal force, fighting at machine speed can dramatically increase the pace of operations.

There are several applications of AI currently in development or are at early stages. The neural networks can utilize imagery databases and classify scenes, allows for a more accurate assessment of specific locations. The processing power that is possible with narrow AI systems [47] have the potential to increase the speed of data analysis. Image recognition can achieve faster, more accurate results than humans can achieve today.

AI and ML can also help in that information gathering and decision-making process.

Successful implementation of AI might lead to new concepts of operation that could influence force structure and force employment, or how professionals organize themselves and plan operations. One possibility is the use of large numbers of smaller platforms for different operations, known as swarms. The algorithms and control systems designed to enable 'swarming' already there are in different sectors and in academia. Expensive, high quality platforms could become vulnerable to swarms of sensors and lower-cost weapons platforms that are effectively networked together. AI could thus help bring quantity back into the equation in the form of large numbers of robotic systems.

Another potential application for AI that could shape the character of conflict is coordination through layers of algorithms that work together to help manage complex operations. AI could accelerate trends that challenge these long running force structure imperatives, such as the need to defeat adversaries with advanced anti access, area denial (A2/AD) networks with tolerable costs.

All the modern armed forces face the same challenge. According to [24] despite spending billions in upgrading existing capabilities, very few of these platforms were designed to seamlessly integrate AI or partner with autonomous robotic systems. This means retrofitting is required, making emergent technology an integration problem. It is also likely to take significant time and effort for the professionals to adapt entrenched command and control approaches to absorb the shock generated by the introduction of artificial intelligence and autonomous systems [17]. AI, autonomous machines are almost certain to create new integration challenges.

According to [24] "*despite some rapid advances in AI development, it is estimated that it could take until 2060-2070 for it to reach the level of maturity required to satisfy many imagined military purposes*."

4. Human-machine teams in future asymmetric operations

In a study done by Center for Strategic and Budgetary Assessments (CSBA) and Mick Ryan (Australian Army) it stands out: "*By the middle of the 21st century, ground forces will employ tens of thousands of robots, and the decisions of human commanders will be shaped by artificial intelligence. Although the future is impossible to predict, trends in technology and warfare make this a near certainty. Military organizations must plan now for this new era of warfare. Governments must be prepared for the political, strategic, and ethical dimensions of this shift in the character of war."* [32]

Many governments and organizations have attempted to identify prevailing trends that will drive or influence strategy and national policy. Likewise, military organizations around the world are studying the changing character of war to inform force structure and procurement decisions. The uncertainty of the future security environment leads to more confusion and no precise predictions of the future. Prudence demands that governments and military organizations outline a range of expected future scenarios based on prevailing trends to inform their planning.

Assessments of the future security environment from Canada, the United States, the United Kingdom, Australia, and New Zealand [48, 49, 50, 51, 52, 53, 54] refers to several common themes and significant changes in demographics and urbanization, geopolitics, economics, the role of the state, the diffusion of power, climate, and resources. Also, emerging, and disruptive technology are forecasted. It is expected that these will not only affect the policy and strategy of nations but will also drive changes in the character of war and future ground force operations.

As mentioned in a Science and Technology Options Assessment Study [55]: "*in the EU there are currently many ongoing efforts towards the improvement of cybersecurity."* The mentioned study concludes that the use of a cybercapability maturity model is necessary for the coherent monitoring and further development of cybercapacities in the Common Security and Defence Policy (CDSP). *"Modelling is important, not only for covering all aspects of cybersecurity, but also for monitoring the maturity of efforts and diverting resources to the areas that need it most. In the CSDP context, there are additional factors that need to be considered for the protection of military and civilian missions, personnel, and infrastructures. The geographical dispersion of CSDP missions beyond the EU borders, the global nature of the threat agents, hybrid threats and the protection of deployed assets from cyberattacks are all challenges that require attention*."

According to [32] *although there are many trends, three key areas of change will most likely affect future ground forces the most: geopolitics, the changing nature of work, and the disruptive impact of robotics and AI.*

All these tendencies are interdependent and potentiate each other so that e.g., the change in the global civilian labour market will eventually affect military personnel management models. New technologies will permit the automation of many tasks currently performed by humans. As automation and AI allow civilian business leaders to place humans in different kinds of work, so too will military personnel planners be forced to think anew about the recruiting and employment opportunities of a new global workforce approach. It is likely to drive the creation of new military personnel models and in turn the designing of new ground force structures. This, along with the disruptive technologies of robotics, AI, and human augmentation could enable new operating concepts.

In addition to expected future geopolitical changes and new global approaches to workforce structures, the potential applications of robotics and AI will drive their military employment. The professionals will be necessary to pay attention to few aspects to describe the key drivers for forces to develop their future human-machine organizations. It is estimated that the teaming humans with robotic and AI capabilities can boost national military power and can improve individual and team performance while reducing threats to humans; military forces could employ robots on future asymmetric operations as an ethical preference; in their turn, future adversaries will use these technologies; robots and AI can improve all institutional and support functions of those forces.

The world is facing unprecedented effort in the development and adopting of AI and ML and undoubtedly recent advances in artificial opened a new universe of opportunities in asymmetric operations. Tasks once believed to mandate human intervention have since been surpassed by machine execution.

Problems once computationally complex infeasible can now be solved in near real-time. It still struggles to understand how to apply AI and ML in a safe, practical, and usable way.

One of the greatest challenges that slow down the use of AI/ML is how to fit the human and machine together. Human-Machine Teaming (HMT) is the concept at which humans and machines intersect and work together toward a common goal. For this partnership to be successful, it is need better insight, context, and explainability - not only for the human to understand the machine, but also reciprocally, for the machine to understand the human. The strengths and weaknesses of both the human and as well as machine must be identified so that it can be understand how the human and machine should communicate, reconcile differences, and agree on a conclusion. In other words, it

must be very well understood how to establish and maintain a common area between people and machines to achieve operational goals [1].

Another approach is by understanding how humans interact with different levels of automated technology [34]. While not all automation will meet the criteria for intelligent teammates, across asymmetric operations such as cyber defense many automated components are limited forms of adaptable automation; that is, they have low adaptability (they are all or none; on or off), or the adaptability is overly time consuming [33]. According [19] it is known in other applications that the development of a more intelligent, responsive, and contextualized teammate, or adaptive automation system, may offer a set of advantages. However, to date, there has been limited exploration of these types of systems as cybersecurity [3].

One of the questions refer to what does it mean for humans and machines to work together effectively on complex analytic tasks? Is human-human teaming the right analogue for this kind of human-machine interaction? Recent works [15], focuses on what behaviors are necessary that allow next-generation intelligent assistants to provide context-sensitive, proactive support for human analytic work - especially as teammates in a cybersecurity asymmetric operational environment. Many of these requirements are like other analytic work: awareness and understanding of a user's current goals and activities, the ability to generate flexible responses to abstractly formulated needs, and the capacity to learn from and adapt to changing circumstances.

To achieve these behaviors, intelligent teammates require processes of coordination and communication that are reminiscent of but distinguishable from those observed in human teams [28]. Teams in cybersecurity operations, especially those in operations centers have specific dynamics that are affected as much by context as they are by the operational environment [29]. If anything, context is the most important challenge to overcome. As work on intelligent agents continues, raises awareness of an over-reliance on human-human teaming constructs and use 'teaming' as a model on which to guide the work in human-machine teaming rather than a set of rules to define it.

Concerning the challenges referring to how machines to understand to provide effective decision support to human, they must be built on cognitive and behavioral models. According to [12] some efforts in user-centered design for cybersecurity have effectively incorporated solutions for decision support needs derived from cognitive work or task analyses.

But all these can fail by not evolving to meet changing human decision-making needs. There are more requests for tools within the machine systems that track human behavior, particularly changes in behavior together with changes in tasks or goals, and then adapt machines to those changes.

Cognitive models could provide the needed solutions [4]. Because they are formal representations, they can be integrated with other intelligent computational algorithms to directly inform the machine about the user [21] and they can further translate machine analytics into human-interpretable actions or representations in an interface.

Integrating these functions, the cognitive models can help adapt the machine behavior to meet evolving human needs, including adapting information for faster decisions, mitigating workload and fatigue, and potentially even acting autonomously, when necessary, to maintain team performance [5].

Since 2013, in [11] it was remarked that many of today's cyberattacks are the result of employee susceptibility to phishing and spear phishing attacks. These cyber attackers exploit human cognitive biases and emotions that can overrule more rational decision-making. Some proponents of the dual process model believe that this less rational heuristic-based decision-making is the default decision-making process.

It may be that the framework described in [27] which tied automation to human information processing, can be extended to cyber kill chains. Combined with task analyses, on the attacker side can develop a better understanding of how humans use existing capabilities along the

"reconnaissance, weaponization, delivery, exploitation, installation, C2, and action" phases [18], and examine how AI could be coordinating and planning alongside the human. For defenders, AI could focus on elements of detection, denial, disruption, degradation, deception, and containment procedures, in addition to the utility of automation for managing updates and patching. Potential must be weighed and measured against foreseeable negative interactions. Ironic results of implementing automation, including creating more (not less) work for humans, failing to decrease required manpower, de-skilling operators, reducing awareness, contributing to accidents and loss of life, and general changing of operator skill and demands must all be considered [2], [35], [14]. In the future, HMT will likely play a larger role in cybersecurity as part of an expert cybersecurity HMT consistently evaluating the network for vulnerabilities. Machines can play a useful role as part of an expert cybersecurity team. However, machines may also play a role in working directly with the average employee to keep him/her safe from cyberattacks. Perhaps this HMT is designed primarily to support task work but can also help prevent cyberattacks by providing decision support.

As Nathan Bos mentioned in [28], a teammate also has the capability to become a liability. It can be extended this further to two specific types of attacks. For example, the important decision making resides in the human, while most of the information gathering and analysis rests within the machine, the combination is an HMT highly vulnerable to integrity attacks (a disruption in the information viewed by the agent), and availability attacks (a disruption of the general operational ability to interact with the teammate, and for the AI to do its work). Adversarial ML will further and uniquely exploit security done by machines. Careless AI teammates could create a cybersecurity irony of automation: a system added to strengthen security, weakens it.

What to do now? A common language and accurate representations will go a long way toward improving the system and human interactions with AI as Cleotilde Gonzalez point in [28]. The combinations of allocation decisions within future HMT are huge, and unfeasible to evaluate in masse [16] even for the kill chain ideas proposed. In [34] noted the best configurations will be through trial and error. Also, modelling, as Leslie Blaha remarks to [28]. Design of AI must avoid the history of ironies known to be fatal to man and mission.

5. Instead of conclusions

There is a great potential for IoT technologies to revolutionize modern warfare, leveraging data and automation to deliver greater lethality and survivability to the warfighter while reducing cost and increasing efficiency. The development and deployment of IoT technologies across the modern-day battlefield requires many challenges to be solved.

Major trends include artificial intelligence (AI), robotics, and the internet of things (IoT) to optimize defense operations and augment military efficiency. Today, conventional warfare is increasingly being replaced by hybrid approaches that also combine cyber warfare and other frontiers. Emerging military technology trends are changing the battlefield in four aspects-connectivity, lethality, autonomy, and sustainability. Connectivity solutions address concerns about how combatants detect and locate their adversaries, communicate with each other, and direct operations.

Future research will need to prove that there are correct models in human decision making in asymmetric operations, especially in cybersecurity, so that they can be incorporated into existing machines and show how machine analytics and cognitive models are integrated. Several additional questions continue to arise regarding the degree to which cybersecurity can be addressed and understood.

In [28] noted that applied behavioral research in cybersecurity could be a focal point of research much more than it currently is. While large sums of money are being spent on both technology and personnel in this area, there has been relatively little research with any behavioral component.

From Nathan Bos vantage point [29], there are three high potential and under-researched topics:

- Information search. The observations of cyber defenders show that information search is a basic activity for many tasks beyond incident response. According to [31] search patterns do not necessarily resemble hypothesis-driven search patterns but are often better characterized as information foraging.
- Judgement with uncertainty and risk. Some systems have been conceptualized such that machines provide intelligence while humans perform the higher-order task of assessing risk, providing judgment, and making decisions under uncertainty. This arrangement is rapidly being re-negotiated, however, as new systems automate risk assessment, and make decisions according to rules both learned and inferred.
- Workforce development. The urgent need for a cyber workforce has led to many undocumented initiatives in recruitment, selection, training, and retraining. This could be a generational problem in educational research if it were understood as such. Of particular interest is the topic of retraining. This happens when staff from quite different specializations are retrained in cybersecurity and when busy professionals try to keep up with an unusually fast-moving field and simultaneously manage the moving interface between human cognition and intelligent tools.

References

[1] Baber, C., Cook, K., Attfield, S., Blaha, L. M., Endert, A., & Franklin, L., 2018, A conceptual model for mixed-initiative sensemaking. ACM SIGCHI Sensemaking Workshop.

[2] Bainbridge, L., 1983, Ironies of automation. Automatica, 19(6), 775-779.

[3] Ben-Asher, N., Oltramari, A., Erbacher, R., & Gonzalez, C., 2015, Ontology-based Adaptive Systems of Cyber Defense. International Conference on Semantic Technology for Intelligence, Defense, and Security, 34-41.

[4] Blaha, L. M., 2018, Interactive OODA processes for operational joint human-machine intelligence. NATO IST-160 Specialist's Meeting: Big Data and Military Decision Making. Bordeaux, France.

[5] Blaha, L. M., Fisher, C. R., Walsh, M. W., Veksler, B. Z., & Gunzelmann, G., 2016, Real-time fatigue monitoring with computational cognitive models. International Conference on Augmented Cognition, 299-310.

[6] Bognár E. K., 2018, Possibilities and security challenges of using IoT for military purposes, Hadmérnök (XIII) 1II (2018), https://www.researchgate.net/publication/336253176_Possibilities_and_security_challenges_of_using_IoT_for_military_purposes, accessed on April 30, 2021.

[7] *GovTribe, 2017, "Internet of Battlefield Things (IoBT) Collaborative Research Alliance (CRA)". April 5, 2017.*

[8] Davison, Neil, 2018, "Autonomous weapon systems under international humanitarian law", https://www.icrc.org/en/document/autonomous-weapon-systems-under-international-humanitarian-law, accessed on April 1, 2022.

[9] Dear, Keith, 2019, Artificial Intelligence and Decision-Making, RUSI Journal, 29 November 2019Emmitt, John, 2021, The Evolution of Automation Technologies, https://www.kaseya.com/blog/2021/02/16/the-evolution-of-automation-technologies/, accessed on April 1, 2022.

[10] Emmitt, John, 2021, The Evolution of Automation Technologies, https://www.kaseya.com/blog/2021/02/16/the-evolution-of-automation-technologies/, accessed on April 1, 2022.

[11] Evans, J. B. & Stanovich, K. E. (2013). Dual-process theories of higher cognition: Advancing the debate. Perspectives on Psychological Science, 8, 223-241.

[12] Franklin, L., Pirrung, M., Blaha, L., Dowling, M., & Feng, M., 2017. Toward a visualization-supported workflow for cyber alert management using threat models and human-centered design. IEEE Symposium on Visualization for Cyber Security, 1-8.

[13] Freedberg Jr., Sydney J., 2017, "War without Fear: DepSecDef Work on How AI Changes Conflict," Breaking Defense, May 31, 2017.

[14] Gutzwiller, R. S., Clegg, B. A., & Blitch, J. G., 2013, Part-task training in the context of automation: Current and future directions. American Journal of Psychology, 126(4), 417-432.

[15] Haimson, C., Paul, C. L., Nebesh, B., Joseph, S., & Rohrer, R., 2019, Do we need "teaming" to team with a Machine? HCI International Workshop on Human-Machine Teaming.

[16] Hancock, P., Mouloua, M., Gilson, R., Szalma, J., and Oron-Gilad, T., 2007, Provocation: Is the UAV Control Ratio the Right Question? Ergonomics in Design, 7, 30-31.

[17] Hoffman, F. G., 2017, Will War's Nature Change in the Seventh Military Revolution?, Parameters 47(4) Winter 2017-18Kott, Alexander; Swami, Ananthram; West, Bruce (December 25, 2017). "The Internet of Battle Things". Computer. 49 (12): 70-75.

[18] Hutchins, E., Cloppert, M., and Amin, R., 2011, Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. International Conference on Information Warfare & Security, 113-125.

[19] Kaber, David B., 2018, A conceptual framework of autonomous and automated agents, Theoretical Issues in Ergonomics Science, 19(4), 406-430.

[20] Kott, Alexander; Swami, Ananthram; West, Bruce, 2017, "The Internet of Battle Things". Computer. 49 (12): 70-75, December 25, 2017.

[21] Lebiere, C., Jentsch, F., and Ososky, S., 2013, Cognitive models of decision-making processes for human-robot interaction. International Conference on Virtual, Augmented and Mixed Reality, 285-294.

[22] Liebermann, Oren, 2021, Lloyd Austin, Defense secretary lays out vision of future in first major speech, CNN Updated 0049 GMT (0849 HKT) May 1, 2021, https://edition.cnn.com/2021/04/30/politics/defense-secretary-lloyd-austin-speech/index.html, accessed on May 1, 2021.

[23] Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions), https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

[24] Mallick, P. K., 2019, Is AI Changing the nature of War?, https://www.vifindia.org/article/2019/january/18/is-artificial-intelligence-changing-the-nature-of-war, accessed on April 2, 2022.

[25] McFadden, C., 2018, A Brief History of Military Robots Including Autonomous Systems, https://interestingengineering.com/a-brief-history-of-military-robots-including-autonomous-systems, accessed on April 2, 2022.

[26] McMillan, Rob, "Definition: Threat Intelligence", Technology Research, May 16, 2013, accessed April 2, 2022.

[27] Parasuraman, R., Sheridan, T.B. and Wickens, C.D., 2000, A model for types and levels of human interaction with automation. IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, 30(3), 286-297.

[28] Paul, Celeste Lyn, Leslie Blaha, Nathan Bos, Robert S. Gutzwiller, 2019, Opportunities and Challenges for Human-Machine Teaming in Cybersecurity Operations, Proceedings of the Human Factors and Ergonomics Society 2019 Annual, available at:

https://www.researchgate.net/publication/334836878_Opportunities_and_Challenges_for_Human-Machine_Teaming_in_Cybersecurity_Operations, accessed on April 1, 2022.

[29] Paul, C. L., 2014, Human-centered study of a Network Operations Center: Experience report and lessons learned. ACM CCS Workshop on Security Information Workers, 39-42.

[30] Pégulu, Marc, 2021, How the Internet of Things is Shifting the Digital Age, https://www.rtinsights.com/how-the-internet-of-things-is-shifting-the-digital-age/, accessed on April 2, 2022.

[31] Pirolli, P. and Card, S., 1999, Information foraging, Psychological Review, 106(4), 643-6.

[32] Ryan, Mick, 2018, Human-Machine Teaming for Future Ground Forces, https://csbaonline.org/research/publications/human-machine-teaming-for-future-ground-forces, accessed on April 2, 2022.

[33] Scerbo, M. W., 1996, Theoretical perspectives on adaptive automation. In R. Parasuraman & M. Mouloua (Eds.), Automation and Human Performance: Theory and Applications. Mahwah, NJ: Erlbaum, 37-63.

[34] Sheridan, T. B., 2017, Comments on "Issues in human-automation interaction modeling: Presumptive aspects of frameworks of types and levels of automation" by David B. Kaber. Journal of Cognitive Engineering and Decision Making, 12(1), 25-28.

[35] Strauch, B., 2017, Ironies of automation: Still unresolved after all these years. IEEE Transactions on Human-Machine Systems, 48(5), 419-433.

[36] CRS Report R45178, Artificial Intelligence and National Security, by Daniel S. Hoadley and Nathan J. Lucas and Peter Singer; "Getting to Grips with Military Robots," The Economist, January 25, 2018; and Aaron Mehta, "AI Makes Mattis Question Fundamental Beliefs About War," C4ISRnet.com, February 17, 2018.

[37] Gartner Top Strategic Technology Trends for 2021, https://www.gartner.com/smarterwithgartner/gartner-top-strategic-technology-trends-for- 2021/.

[38] Gartner Identifies the Top 10 Strategic Technology Trends for 2020, https://www.gartner.com/en/newsroom/press-releases/2019-10-21-gartner-identifies-the-top-10-strategic-technology-trends-for-2020).

[39] Gartner Says AI Augmentation Will Create $2.9 Trillion of Business Value in 2021, https://www.gartner.com/newsroom/press-releases/2019-08-05-gartner-says-ai-augmentation-will-create-2point9-trillion-of-business-value-in-2021.

[40] Kaseya® is the leading provider of IT and security management solutions for managed service providers (MSPs) and small to medium sized businesses (SMBs), www.kaseya.com.

[41] Gartner Top Strategic Technology Trends for 2021, https://youtu.be/s3rlYWcwdDY.

[42] CTIPs: What is Cyber Threat Intelligence and how is it used? (https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf, accessed on April 2, 2022.

[43] The Recorded Future Team, September 13, 2018, How Strategic Threat Intelligence Informs Better Security Decisions, https://www.recordedfuture.com/strategic-threat-intelligence/.

[44] The Recorded Future Team, September 19, 2018, How Tactical Threat Intelligence Helps Identify the Enemy, https://www.recordedfuture.com/tactical-threat-intelligence/.

[45] The Recorded Future Team, September 25, 2018, How Operational Threat Intelligence Blocks Attacks Before They Happen, https://www.recordedfuture.com/operational-threat-intelligence/.

[46] Artificial Intelligence Market Statistics: 2025, https://www.alliedmarketresearch.com/artificial-intelligence-market.

[47] Ben Dickson, 2020, What is artificial narrow intelligence (Narrow AI)?, https://bdtechtalks.com/2020/04/09/what-is-narrow-artificial-intelligence-ani/#:~:text=Narrow%20AI%20is%20the%20umbrella%20term%20that%20encompasses,that%20falls%20outside%20their%20problem%20space%2C%20they%20fail.

[48] Ministry of Defence (MOD) UK, Global Strategic Trends-Out to 2045 (Shrivenham, UK: Development, Concepts and Doctrine Centre, June 30, 2014).

[49] MOD UK, Future Operating Environment 2035 (Shrivenham, UK: Development, Concepts and Doctrine Centre [DCDC], December 14, 2015).

[50] David T. Miller, Defense 2045: Assessing the Future Security Environment and Implications for Defense Policy Makers (Washington, DC: Center for Strategic and International Studies, November 2015).

[51] Directorate of Future Land Warfare, Future Land Warfare Report (Canberra: Australian Army Headquarters, 2014).

[52] Army General Staff, Future Land Operating Concept 2035: Integrated Land Missions (Wellington, NZ: Headquarters New Zealand Defence Force, 2017).

[53] Vice Chief of Defence Force, Australia, Future Operating Environment 2035 (Canberra: Commonwealth of Australia, 2016).

[54] Canadian Department of National Defence, Designing Canada's Army of Tomorrow: A Land Operations 2021 Publication (Kingston, Canada: Directorate of Land Concepts and Designs, 2011).

[55] Cybersecurity in the EU Common Security and Defence Policy (CSDP). Challenges and risks for the EU., 2017, European Parliamentary Research Service Scientific Foresight Unit (STOA) PE, ISBN 978-92-846-1058-7.