Possibilities and Limits of a C2 (R)Evolution

By Lieutenant Colonel Andreas Schmidt, GE AF, JAPCC

Introduction

Military planners often focus on the development of individual capabilities without considering how they will work in concert with the rest of a nation's forces or let alone allied forces. As with any fine symphony orchestra, harmonizing these capabilities requires a world-class conductor. Command and Control (C2) systems – and their operators – are the military equivalent of the conductor. It is intuitive that an improved C2 system can increase military efficiency and effectiveness, comparable to the orchestra playing more swiftly and striving for the perfect performance. However, what is actually considered a C2 improvement

and how will such *improvements* be judged? Is it simply that a new C2 system can be considered better if the cost/benefit ratio at the strategic level is *improved* while controlling the same effect-delivering tools, or does *improvement* involve more aspects? The main factors for such improvements could be an increase of overall speed and a decrease in friendly force attrition. Assuming that the outcome of a fair one-on-one duel between two competing systems at the tactical level is a relatively statistical coin toss, this *fair* balance needs to be influenced by the advantages gained from the tactical to the strategic levels. The following will look at some options and their benefits, as well as their drawbacks.

Situational Awareness

One way to skew the balance and improve the effect-delivery of individual systems is to achieve better Situational Awareness (SA) than the opposing systems, which should enable optimized and faster decisions. This requires that all necessary information is available in time for each process (e.g. planning, deployment, engagement) to create an advantage. This is often also called *information superiority.*[1] The sheer amount of active and passive sensors (including both technical and human) available to NATO and its nations, from all domains, produce massive volumes of data. The next steps are converting data to information and then possibly to knowledge,[2] followed by its dissemination to the required users. Hypothetically, assuming that the continuous data and information sharing of national sources is given, it needs to be decided what can, will, and must be delivered, and to whom. The knowledge to information conversion before transmission requires trust, but also needs to utilize less bandwidth to save time when serving more than one user. Trust applied to digital content is sometimes referred to as *e-trust.*[3] However, this reduces the options for context analysis by a local commander/operator, which, in turn, emphasizes the need for data/information veracity. Additionally, the more data/information that is available, the more imperative 'what is relevant' must be determined to create the advantage. Practically, this can only be done closer to the point of collection, unless the client knows exactly what he actually needs. This becomes less likely with the growing amount of available material, amplified by the bottleneck of distribution through existing networks. In addition, with the increasing volume of data, the actual need for computerized analytical support increases, which is true for detection, classification, identification, and the categorization of relevant data. This is where the constantly evolving fields of Artificial Intelligence (AI),[4] Big Data,[5] Deep Learning,[6] and Quantum Computing[7] can help to increase speed and efficiency.

Such enhanced efficiency also has its drawbacks. Not only do we have to think about, and deal with, new types of misinformation, since it has a different meaning for an AI than for the human operator,[8] but also the potential final recipients of the misinformation need to be trained accordingly. The human decision-making process is based on two types of reasoning: 1) more time-consuming deliberative reasoning, and 2) automatic reasoning for routine decisions. Studies have shown that humans tend to use more automatic reasoning when interacting with automated systems.[9] The faster the system, the less likely the operator will use deliberative reasoning. The debate about *killer robots*[10] revolves around automated or autonomous decisions, lacking the meaningful human control when using lethal force. This can be avoided by keeping these decisions in human hands. However, if the operator is not well trained, there could be little difference in the outcomes in some instances.

To use Surface-Based Air and Missile Defence (SBAMD) systems as an example, external cueing data allows for optimized emissions control and, therefore, later radiation detection and fewer electronic countermeasures. This also supports the optimization of intercept points and the employment of advanced fire

© MCD, Hille Hillinga

control concepts[11] like engage- or launch-on-remote. However, following several fratricide incidents by SBAMD units in Operation Iraqi Freedom, a United States Department of Defense report[12] stated three shortfalls, which led to these sometimes-fatal circumstances. Firstly, critical identification systems performed poorly; secondly, there was a significant lack of SA in the air defence systems; thirdly, the SBAMD concept of operations did not match the actual operational conditions, yet the operators were trained to trust the system. This supports the notion that technical options need to go hand in hand with operational requirements and, most importantly, adequate training.

System of Systems in a Multi-Domain Environment

The overall efficacy of a military action relies on the capabilities used and the way they are employed. Enhancing either will surely improve the outcome. However, just optimizing existing capabilities and processes will have limits, e.g. technical limitations or procedural insufficiencies, to achieve the necessary effect. This might necessitate the development of completely new approaches or capabilities. In the end, the result needs to deliver the envisioned benefits whilst remaining robust for contingency circumstances.

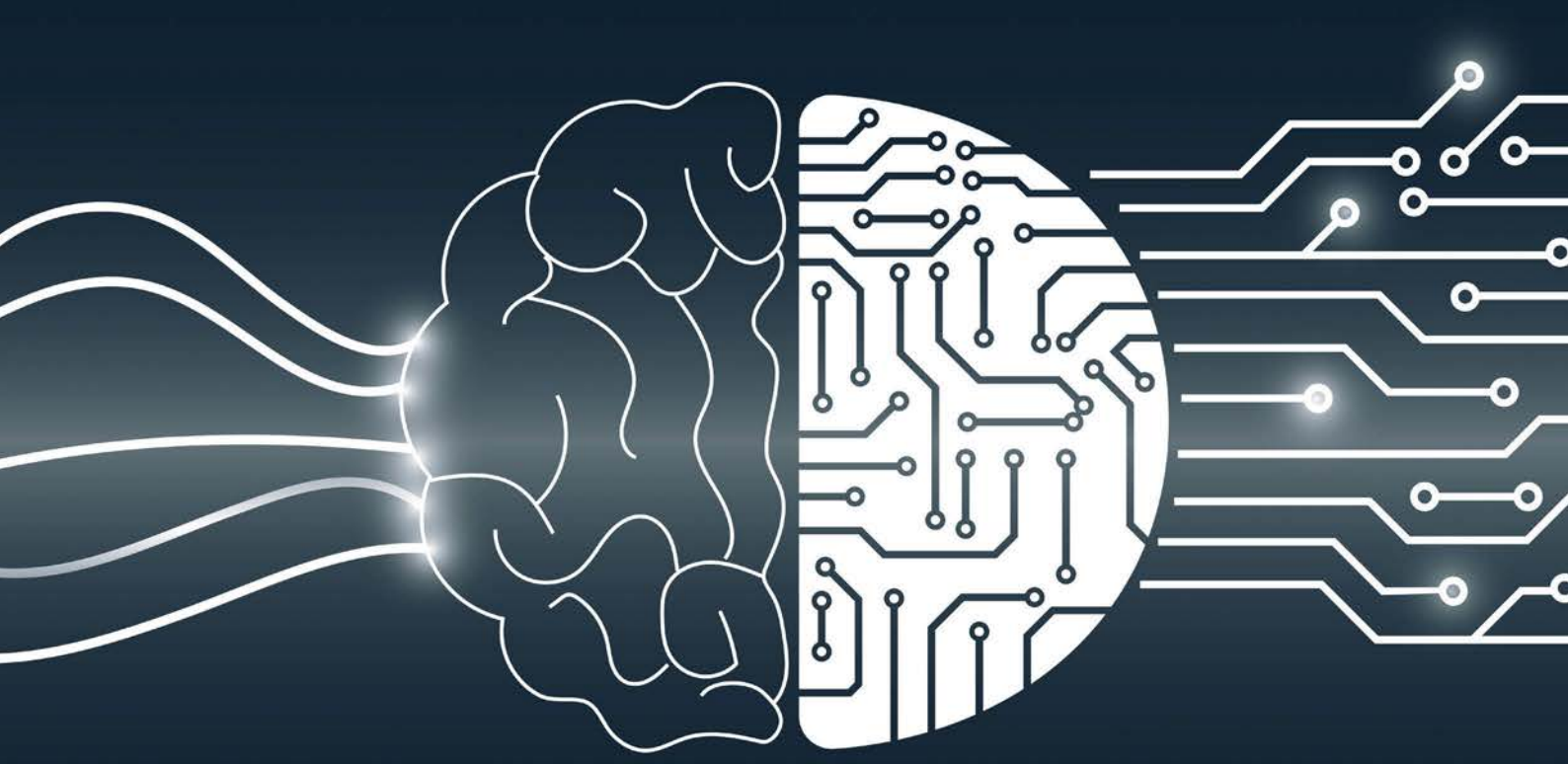
One-on-one or one-on-many engagements are the individual puzzle pieces of every military confrontation, however, the overall purpose is to achieve a desired strategic end-state when using military force.[13] Aside from individual system effectiveness, the art of military operations is to employ the selected military forces in concert to create overall advantage. At the operational/tactical level, the goal is to employ individual systems as synergistically as possible. Over the recent decades, the significantly increased SA has allowed military operations to switch from a more attrition-focused approach to a more effects-based idea. Furthermore, the ability to network military forces allows for increasingly dynamic joint and combined operations. In current NATO operations, a Joint Force Component leads the individual domain components (e.g. Joint Force Air Component), which provide capabilities in their respective domains. This necessitates, for example, the robust joint coordination of combined forces for target and protected assets prioritization, while still employing a domain-centric focus on effect-delivery itself. In this regard, a SBAMD unit, led by the air component, can provide coverage of an asset requested by the land component, or receive land or naval support for offence-defence integration. Despite joint coordination, domain planning remains mostly at the domain component level. One method to gain an advantage is to plan and execute faster than the opponent's planning cycle, denying the adversary an opportunity for optimal execution. The better the overall SA, the better the military planner can define and understand the *problem space.*[14] All of our available

effects, which will help transform the *problem space* into our desired end-state, can be considered the *solution space*.

When thinking in terms of effects, the anticipated odds of applying an effect successfully needs to be maximized. There are two ways of achieving this: by using new weapons, like hypersonic glide vehicles, which promise a high probability of success by exploiting adversary capability gaps, or by combining various capabilities from one or more domains to degrade an effective countermeasure. Every delivered effect changes our *problem space,* which has a subsequent effect on our plans. Currently, air operations and associated air tasking orders are typically planned and executed in 72-hour cycles, allowing for adaptation to *problem space* changes.[15] Other component commands have different planning cycles, which are synchronized at the joint level. With optimal *problem and solution space* awareness at the joint level, supported by available networks and modern software tools, this process can be streamlined to reduce the length of planning cycles and to include solutions with a more robust use of effects from multiple domains towards one objective with less extensive coordination. In addition, the relationship between supporting and supported units should become more flexible in multi-effect missions, since the chosen command relationship construct could be ad-hoc, effect-dependent, and less long-term mission centric. This even more centralized planning and decentralized execution will further transform domain components into mostly capability custodians and effect providers. The military *decision space* will move up in the C2 hierarchy, with the lowest level military entity planned to be the provider or contributor of a *robust* effect, while *robust* has to be defined from a multi-domain viewpoint. This might also have an impact on which and how nations contribute forces to NATO operations, since the ad-hoc, agile force planning can be stymied by the national *red-card holder* concept.[16] For execution, at the tactical level, the magnitude of the change is dependent on the versatility of the tactical capability in affecting the battlespace and providing broader effects. Highly mobile air assets, especially those with a wide spectrum of payloads for various effects, could be used even more flexibly and effectively than before. SBAMD systems, in general, will benefit greatly from improved SA, resulting in optimized firing and emissions control doctrines, better shot management of layered defences and an overall better use of the defensive inventory. However, the level of unit mobility will have a significant impact on the added value for flexible employment decisions. Long-range SBAMD units have relatively low mobility, which won't allow for very rapid, long-distance redeployments to cover ad-hoc mission changes. Short-range SBAMD units, however, have higher mobility and will be able to provide coverage in a more flexible way. With significantly increased SA and enhanced planning and execution tools (e.g. AI-enabled) at the joint level, it could be possible to bring a construct like Joint All-Domain Operations[17] to life. This could, in turn, enable faster planning-to-execution cycles, multi-domain dilemmas for the opponent and concentration of an effects-based approach towards the desired end-state. Although it sounds promising, this approach has at least two downsides that must be considered.

Downsides of C2 Relying on Technological Constructs

The development of new C2 constructs based on new technological achievements is not an original idea. We can assume that our potential adversaries are working on similar concepts, also that they are speeding up the operational tempo. Keeping sufficient SA for an adequate understanding of the *problem space* will become more complex. Additionally, our decision cycle must constantly speed up to be able to inject effects into the opponent's planning process. Since the use of human operators itself represents a limiting factor when it comes to processing speed, new C2 constructs have to rely more and more on technological solutions. This might lead to the military equivalent of a *technological singularity,*[18] a *battlefield singularity,*[19] where human cognition can no longer keep up with machine speed. Therefore, by starting the process of speeding up future warfare with the help of computers, AI, or deep learning, we must be aware of the consequences to the overall process. In addition, our ethical and judicial framework must address this dilemma as well. For a moment, let us consider that this challenge can be met and a viable C2 construct of



future warfare created. The human actor/operator, from the political/strategic level down to the tactical level, needs to adapt and train to function in such an environment. Thinking in fast-paced, multi-domain effects terms requires specialized and empowered personnel. Since, from an engineering perspective, it is easier to develop something against an existing capability, it can be assumed that future adversaries will design options to interrupt or negate this new environment. For example, an adversary could use quantum computing to decipher our secure communications, which would significantly impact availability, reliability, and secrecy of data/information. Therefore, a contingency plan needs to be prepared, available, and exercised. This contingency plan requires not only the availability of fall-back technology for planning, execution, and communication, but also the human capacity to remain proficient in both future and *current* C2 constructs. With limited military equipment and available time, this could become a challenge for resource management. A current example is our reliance on Position, Navigation and Timing (PNT) systems such as Global Positioning System (GPS). GPS makes warfare significantly more efficient and effective, but denial of this service is relatively easy using simple tactics such as jamming or spoofing of GPS signals.[20] Therefore, soldiers need to be able to use the benefits of PNT, recognize the potential for interference, but also retain the ability to execute their missions without GPS. A good example of GPS interruption in the SBAMD realm is the accurate emplacement of sensors and shooters for correct engagements and the provision of an unambiguous air picture without PNT service. Therefore, both methods, with and without GPS, constantly have to be practiced. However, the increasing reliance on technological solutions in future complex C2 systems bares similar issues. The overall system needs to be prepared to function under all circumstances. The more robust the underlying technology for future C2 constructs becomes, all-encompassing from core (e.g. Intelligence, Surveillance and Reconnaissance platforms or planning/execution tools) to enabling systems (e.g. communication networks or PNT), the less we have to think about legacies; but this will be costly and time-consuming. Robustness of a system, defined as operating correctly in the presence of exceptional inputs or stressful conditions,[21] can only be tested against all currently imaginable conditions and inputs. Therefore, robustness needs to be continually reassessed and constantly maintained, especially in a rapidly evolving environment.

Conclusion

Technical innovations have always allowed for improvements in military warfare. Still, just because something is technologically feasible, that does not mean it can be incorporated with ease or without side effects. Optimized SA and more capable tools will always allow for better and faster planning and execution. However, this capability needs to be as robust

as possible in all anticipated scenarios, backed by suitable fall-back options. All personnel must be sufficiently educated and trained in both worlds and able to switch seamlessly between the two. Also, the increased speed of military operations, due to technical support, must be balanced with human capabilities in an ethical and legal framework. The more complex systems become, the more emphasis needs to be placed on maintaining robustness and resilience in a constantly evolving environment. It is not about a one-time procurement of a C2 toolkit, rather the constant evolution of systems and the requisite education and training of the operators at all levels. Giving the orchestra some new instruments or a new conductor will certainly require fine-tuning, continuous rehearsal, and a genuine performance review, always with a fall-back option to replicate familiar quality standards to satisfy listener's expectations.

However, there is no real alternative to choosing the path of evolving our C2 systems, because potential opponents will be doing the same and thereby potentially gaining a decisive, hard-to-match advantage. Potential autocratic opponents may have far less restrictive legal and ethical boundaries for the employment of emerging technologies (e.g. AI, deep learning) and can, therefore, field these capabilities unconstrained. Hence, our system not only needs to keep up with this pace, but also needs to be capable of compensating for employment limitations with other means, allowing us to stay competitive. ●

1. Walter Perry, David Signori, John Boon, Exploring Information Superiority, 2004, https://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR1467.pdf (accessed 16 Aug. 2021).
2. Shannon Kempe, The Data – Information – Knowledge Cycle, Nov. 2013, https://www.dataversity.net/the-data-information-knowledge-cycle/# (accessed 16 Aug. 2021).
3. Andrea Ferrario, In AI We Trust Incrementally: a Multi-layer Model of Trust to Analyze Human-Artificial Intelligence Interactions, 2019, https://link.springer.com/article/10.1007/s13347-019-00378-3 (accessed 16 Aug. 2021).
4. Artificial Intelligence, What is it and why it matters, https://www.sas.com/en_us/insights/analytics/what-is-artificial-intelligence.html (accessed 16 Aug. 2021).
5. Big Data: The three Vs explained, https://bigdataldn.com/intelligence/big-data-the-3-vs-explained (accessed 16 Aug. 2021).
6. Machine Learning vs. Deep Learning, https://datasolut.com/machine-learning-vs-deep-learning (accessed 16 Aug. 2021).
7. Homepage IBM, https://www.ibm.com/quantum-computing/what-is-quantum-computing (accessed 16 Aug. 2021).
8. Zach Hughes, Fog, Friction and thinking Machines, Mar. 2020, https://warontherocks.com/2020/03/fog-friction-and-thinking-machines (accessed 16 Aug. 2021).
9. Elke Schwarz, The (im)possibility of meaningful human control for lethal autonomous weapon systems, Aug. 2018, https://blogs.icrc.org/law-and-policy/2018/08/29/im-possibility-meaningful-human-control-lethal-autonomous-weapon-systems (accessed 16 Aug. 2021).
10. Human Rights Watch, https://www.hrw.org/topic/arms/killer-robots (accessed 16 Aug. 2021).
11. Bonnie Young, Future Integrated Fire Control, Jun. 2005, http://www.dodccrp.org/events/10th_ICCRTS/CD/presentations/325.pdf (accessed 16 Aug. 2021).
12. Report of the Defense Science Board Task Force on Patriot System Performance Report Summary, Jan. 2005, https://dsb.cto.mil/reports/2000s/ADA435837.pdf (accessed 16 Aug. 2021).
13. Dr Guy Duczynski, Effects-Based Operations: A Guide for Practitioners, https://www.hsdl.org/?view&did=454767 (accessed 16 Aug. 2021).
14. Ibid. 4.
15. NATO Allied Joint Doctrine AJP 3 for the Conduct of Operations.
16. Katja Lindskov Jacobsen, Rune Saugmann, Optimizing Coalition Air Warfare: the Emergence and Ethical Dilemmas of Red Card Holder Teams, Jun. 2019, https://onlinelibrary.wiley.com/doi/full/10.1111/1758-5899.12670 (accessed 16 August 2021).
17. US Congressional Research Service, Joint All-Domain Command and Control, Mar. 2021, https://fas.org/sgp/crs/natsec/IF11493.pdf (accessed 16 Aug. 2021).
18. Murray Shanahan, The Technological Singularity, Aug. 2015, https://mitpress.mit.edu/books/technological-singularity (accessed 16 Aug. 2021).
19. Elsa B. Kania, Battlefield Singularity, Nov. 2017, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Battlefield-Singularity-November-2017.pdf?mtime=20171129235805&focal=none (accessed 16 Aug. 2021).
20. Victor Rivero Diez, Spoofing and Jamming over GNSS, Jul. 2020, https://www.incibe-cert.es/en/blog/spoofing-and-jamming-over-gnss (accessed 16 Aug. 2021).
21. Zoltán Micskei, Robustness Testing, http://mit.bme.hu/~micskeiz/pages/robustness_testing.html (accessed 16 Aug. 2021).

Lieutenant Colonel Andreas Schmidt

joined the German Air Force in 1993. After attending Officers School, he studied Computer Science at the German Armed Forces University in Munich. Since 1998, he built up an extensive background in Ground Based Air Defence, particularly the PATRIOT weapon system. He started as a Tactical Control Officer and subsequently held positions as Reconnaissance Officer, Battery Executive Officer and Battery Commander in various PATRIOT units. Furthermore, he had two non-consecutive assignments in Fort Bliss, Texas. The main task of his first assignment was to conduct bilateral US-GE studies of weapon system behaviour on a tactical level for the German PATRIOT Office. During his second assignment, he was the Subject Matter Expert (SME) on Integrated Air and Missile Defence at the German Luftwaffe Air Defence Centre. In between, he had an assignment as the A3C in the former Air Force Division. Currently, he is the Integrated Air and Missile Defence/Ballistic Missile Defence SME in the JAPCC.