4 SUMMIT VIENNA 2015 IS4IS

Extended Abstract

„Revolution in Military Affairs“ —

Not without information and communication technology

Hans–Jörg Kreowski[13]* and Dietrich Meyer–Ebrecht [23]

[1] Universität Bremen, Fachbereich 3, Postfach 330440, D-28334 Bremen, Germany

[2] RWTH Aachen, Institute of Imaging and Computer Vision, D-52056 Aachen, Germany

[3] Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF)

E-Mails: kreo@informatik.uni-bremen.de; dme@fiff.de

* Author to whom correspondence should be addressed; Phone: +49-421-218-64451; Fax: +49-421-218-64459

Accepted:

Introduction

In this presentation, we want to discuss the essential and disconcerting role of information and communication technology (ICT) in the current military doctrines and strategies establishing a “Revolution in Military Affairs”.

Life is going to be digital, so is warfare. The concept of Revolution in Military Affairs (RMA) describes how military doctrines and strategies change fundamentally if new military technologies arise. Under President George W. Bush, RMA has become the baseline of defense policy and armament planning of the Unites States (cf. Joint Vision 2010 [1] and Joint Vision 2020 [2]). Its objectives are a global network of battle units including unmanned combat vehicles, precision strikes to minimize collateral effects and remote operations to spare own soldiers lives. The necessary key technologies are computers (synonym for ICT) with ICT–driven weapon development and the further establishment of command-control-communication-intelligence infrastructures (C3I).

Computers and weapon technology: a quick walk through history

First computers came up in the 1940s: Konrad Zuse´s developments financed by Deutsche Wehrmacht; similar military developments in Great Britain and the United States. In the following

three decades after World War 2, the classical case of dual-use dominates: military-driven develop–ment of ICT with rapid evolvement of civil computer applications. Computer professionals became aware of the massive use of computers in weapons not before the 1980s. The political situation in Germany and, in particular, the deployment of Tomahawk (cruise missile, early kind of drone) and Pershing II (ballistic missile) triggered the foundation of FIfF (Forum Computer Professionals for Peace and Social responsibility) in 1984. (See [3,4] for more details.)

Dual-use reversed into its contrary

Today´s military computers and communication systems are mainly based on civil technology. Hardware and software technologies are too complex to be designed from scratch, they need a kind of evolution. The maturing of technology has been based on a myriad of civil applications. ICT–driven weapon technology is inevitably based on civil research and development, resulting in a spreading grey area:

example 1: drones, controlled via global communication networks, vision sensor technology, etc.,

example 2: autonomous unmanned combat vehicles (popularly called killer robots), driving force for RoboCup etc.

Concerning the security euphemism (security research, security architecture, security technology, etc.), industrial strategies and government policies support that the demarcations between civil and military security become blurred:

example 1: integration of the Forschungsgesellschaft für Angewandte Naturwissenschaften (FGAN) in die Fraunhofer-Gesellschaft (FhG) with the establishment of the Fraunhofer Group for Defense and Security, civil and military security research now under one roof, cross-fertilization explicitly intended,

example 2: BMBF (Ministry of Education and Research) research strategy, BMBF and BMVg (Ministry of Defense) minister`s recent statements,

example 3: the European Commission’s security research program (1 400 000 000 €).

The consequences for universities and federal research facilities are that they make profit from trickle–down effect simultaneously undermining civil clauses due to loss of transparency. The consequences for the individual computer professional are the difficulty of reasoning and the uncertainty of taking bearing in their professional environment. (Confer [5,6].)

Intrinsic challenges of ICT-based weapon systems and military infrastructures

Complexity and invisibility of embedded ICT tends to blur public conscience by misinformation and disinformation. Hiding real warfare behind computer screens lowers the threshold for approval. The consequence for global political developments is that weapons with effects remaining under the public perception threshold constitute a grey area of proliferating non-declared wars (e.g. cyber attacks, drone strikes).

example 1: cyber weapons in face of the vulnerability of civil life due to increasing penetration by ICT infrastructures,

example 2: drones from 'civil' applications to stealth missions; excessive pool of ICT inside and behind, inexorable development towards autonomous combat air vehicles.

Evolving technology, driven by research in Artificial Intelligence, is a core business of computer science. The further development of armed robots and robot arms will lead to weapons that decide

autonomously what they destroy and whom they kill. Therefore, a debate on ethics arises unavoidably: Who is responsible? How can the laws of war (like the Geneva Convention) be respected by machines? Is 'computer ethics' an option? (Confer [7,8].)

Message to the concerned computer professional

Stop sleepwalking into a technology-driven "defense" policy, and try to recognize a potential involvement in weapon development, military budget resources etc., contribute to public awareness. Consider to foster a rigorous ban of all weapon systems which shirk public control like is demanded for autonomous combat vehicles by the International Committee for Robot Arms Control (ICRAC). Unveil the abuse of the dual-use term, and employ your expert knowledge to enhance public awareness.

A more elaborated discussion can be found in [9].

References

1. Department of Defense (USA): Joint Vision 2010, 1996, http://www.dtic.mil/jv2010/jv2010.pdf
2. Department of Defense (USA): Joint Vision 2020, 2000, http://www.dtic.mil/doctrine/concepts/ccjo_jointforce2020.pdf
3. Bickenbach, J., Keil-Slawik, R.; Löwe, M.; Wilhelm, R. (Eds.) *Militarisierte Informatik*, Schriftenreihe Wissenschaft und Frieden 4, Berlin, 1985.
4. Kreowski, H.-J. Informatik und Militär: Zusammen in den Abgrund, In *Umdenken in der Informatik*, *2. Jahrestagung des Forums Informatiker für Frieden und gesellschaftliche Verantwortung 1986.*, Löwe, M.; Schmidt, G.; Wilhelm, R., Eds., Verlag für Ausbildung und Studium in der Elefanten Press, Berlin, 1987, pp. 37-42, reprint in *FIfF-Kommunikation* **2011**, 4, pp. 51–54.
5. Meyer-Ebrecht, D.: Dual-use und die Zivilklausel: ‚Sicherheitsforschung' – oder wie Rüstungsforschung zivile Forschung vereinnahmt. *FIfF-Kommunikation* **2012**, 4, pp. 56–58.
6. Töpfer, E. Zivil-militärische Sicherheitsforschung. *Wissenschaft und Frieden* **2012**, 4, pp. 16–19
7. Arkin, R.C. Lethal Behavior in Autonomous Robots, Chapman & Hall/CRC 2009
8. Kreowski, H.-J.: Gehören Killerroboter vor ein Kriegsgericht?, *FIfF-Kommunikation* **2011** 28,4, pp. 27-29.
9. Kreowski, H.-J.; Meyer-Ebrecht, D. Der Missbrauch der Informationstechnik für die ‚Revolution' des Kriegsgeschäfts. In *Gesellschaftliche Verantwortung in der digital vernetzten Welt*, Bittner, P.; Hügel, S.; Kreowski, H.-J.; Meyer-Ebrecht, D.; Schinzel, B. , Eds., LIT Verlag, Münster, 1914, pp. 81 – 88.