SigInt 2013, 5.—6. July 2013

„Revolution in Military Affairs“ — Why computer professionals should be concerned

Hans–Jörg Kreowski and Dietrich Meyer–Ebrecht,
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF)

We will discuss the essential and disconcerting role of information and communication technology (ICT) in the current military doctrines and strategies spoken of as the 'Revolution in Military Affairs' or RMA. We will draw the line from the origin of computers as a genuine dual-use technology towards today's amalgamation of civil and military technologies and its implications for computer professionals.

Synopsis

- Computers and weapon technology: a quick walk through history
- Dual-use reversed into its contrary: technological pull and political push
- Civil vs. military technologies – a grey area: implications for research and development, policy and society
- ICT-based weapons fostering evolvement of a grey area between peace and war
- Current developments of concern: cyber weapons, killer drones, armed robots …
- Ethical issues -- who takes responsibility?
- Message to the computer community

Key statements

Intro
Life is going to be digital, so is warfare. The concept of Revolution in Military Affairs (RMA) describes how military doctrines and strategies changed fundamentally with the advent of new military technologies. Under President George W. Bush, RMA has become the baseline of defense policy and armament planning of the Unites States (cf. Joint Vision 2010 and Joint Vision 2020). 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. Those scenarios are essentially based on computer technology. Key elements are ICT–driven weapon developments and the ongoing establishment of global command-control-communication-intelligence infrastructures (C3I).

History
Computers are a classical case of dual-use technology. While first computer developments in the 1940s were driven by military budgets (Konrad Zuse's work financed by Deutsche Wehrmacht, similar military developments in Great Britain and the United States), civil computer applications evolved rapidly after World War 2. Computer professionals, however, became aware of the ongoing 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) in our backyard triggered the foundation of FIfF in 1984. Meanwhile the exploitation of ICT for military purpose went on. In 1996 the US General Staffs published the so-called Joint Vision 2010 (in 2000 replaced by the Joint Vision 2020), which was essentially calling for a restructuring of the Forces towards employing the entire range ICT-based weapons and C3I-integrated weapon systems. Evolving scenarios of 'new wars' culminated in the Revolution in Military Affairs (RMA) doctrine, which is eventually supplemented by „Obama’s way to war“ meaning the combination of cyber warfare, drones and special forces.

Dual-use reversed into its contrary by intrinsic needs
Today's military computers and communication systems are essentially based on the evolvement of civil technologies. Eventually hardware, software and network technologies had become far too complex to be designed from scratch, they rather needed a long evolution process. Their

maturation has been supported by a myriad of civil applications. Thus, unknowingly, we all paid for military computer applications: Our expenditures in computing and communication equipment justified industry's continuous investments into ever improved manufacturing processes. The other way round ICT–driven weapon technology is inevitably based on civil research and development hence creating a spreading grey area. Examples are drones, controlled via global communication networks, vision sensor technology, etc. Or autonomous unmanned combat vehicles (popularly called killer robots), which are the driving force behind many civil robot research projects, and even contests.

Dual–use reversed into its contrary by policy
Industrial strategies and government policies do their part to blur the demarcations between civil and military security supported by euphemistic parlance such as security research, security architecture, security technology. This is underlined, for example, by the integration of the Forschungsgesellschaft für Angewandte Naturwissenschaften (FGAN), a military research facility, with Fraunhofer-Gesellschaft (FhG) by the establishment of the Fraunhofer Group for Defense and Security Research (VVS) where civil and military security research now are performed under one roof, cross-fertilization explicitly intended. Or the BMBF research strategy demonstrated by BMBF and BMVg ministers' recent statements. Or the European Commission's Security Research Program endowed with the lush budget of 1.4 billion €. Universities and federal research facilities, under an ever increasing pressure to raise third-party funds, are forced to make profit from the trickle-down effect this way undermining civil clauses due to the loss of transparency, even deliberately blurring the real purpose of budgets. Again, we all pay for military R&D, this time with our tax money--apart from that part which is anyway designated to the governmental defense budget. Moreover, computer professionals, if they decline to take their part in military developments, face, to an increasing extent, the difficulty of reasoning and the uncertainty of taking bearing in their professional environment.

Intrinsic perils of ICT-based weapon systems and military infrastructures
The complexity and invisibility of embedded ICT tends to blur public awareness by misinformation and disinformation, with and without deliberation. Hiding real warfare behind computer screens lowers the threshold of public approval for martial engagements. ICT-powered weapon systems unclose the option to keep military operations under the public perception threshold thereby creating a grey area of proliferating non-declared wars. Exemplary means are cyber attacks and drone strikes. Cyber weapons get their threatening potential due to the vulnerability of civil live under the increasing penetration by ICT infrastructures. The transition from cyber crime to cyber warfare is fluently thus posing the problem of attribution of cyber operations. Drones are said to be useful for 'civil' applications as likewise for stealth missions. Hidden to public awareness they feature an excessive pool of ICT inside their body as well as behind their operations. Their nature and purpose implicates an inexorable progression towards autonomous combat air vehicles.

Armed robots and robot arms, technologies to beget nightmares
The development of autonomous systems, driven by research in Artificial Intelligence, is a core business of computer science. Armed robots or robot arms, officially called autonomous combat vehicles, are being developed in a great variety ranging from terrestic vehicles, sea and undersea vessels to aircrafts. Foreseeable, their ongoing development will create weapons that decide autonomously what they shall destroy and whom they shall kill. At this point, a debate on ethics has imperatively to be established among those responsible for technology development and political decisions. Questions like 'Who is responsible?', 'How can the laws of war (like the Geneva Convention) be respected by machines?', 'Are "computer ethics" an option?' have to be answered. Even a rigorous ban of autonomous combat vehicles has to be discussed such as demanded by the International Committee for Robot Arms Control (ICRAC).

Our message to the concerned computer professional
Stop sleepwalking into a technology-driven defense policy, try to recognize your potential involvement in weapon development, try to track back budget resources, unveil the abuse of the dual-use term, employ your expert knowledge to enhance public awareness!