On Facts and Fiction of "Information Warfare"

Ute Bernhardt, Ingo Ruhmann*

Information Warfare has become a keyword for a revolution in military operations with far reaching political consequences, just as well as it is a phrase for pure military science fiction. It is thus necessary to separate the media hype from the development of information technology and its broad use by the military. It is shown how Information Warfare has developed from its origins in the use of computers for command and control, in weapons systems, and from electronical and psychological warfare into a new and comprehensive way of military operations. The political implications of this change are addressed together with the limits to conflict resolution by technical means.

1 Concepts, Meaning and the Media

Just as the preparations for a new war against Iraq are under way (work on this paper was finished in December 2002), the media once again put an emphasis on the use of Information Warfare as a new tool in armed conflict. U.S. officials are praising Information Warfare as "mining of data bases and lots of false targets generated. And, if most of the computers in the country immediately go down, that's not a bad way to start a war"[1].

In these very few words, taken at random from current publications, many of the expectations, misunderstandings, false leads and pure hype coupled with Information Warfare can be identified. A "mining of databases" under ordinary circumstances would rather be interpreted as "data mining", the concept of a complex search process in different data bases. The article, however, continues with descriptions of tools for hacking into adversaries' computers as described in the Department of the Army's Field Manual 100-6 "Information Operations"[2] thus suggesting an offensive meaning of "mining". If we assume that the official interviewed knows the terminology in his field, as a first point, the problems of explaining Information Warfare to the media become obvious.

* FIfF e.V. (Computer Professionals for Peace and Social Responsibility), Goetheplatz 4, D-28203 Bremen, Germany. Email: ute@kriton.bn.shuttle.de, ingo.ruhmann@acm.org

[1] David A. Fulghum: War planning for Iraq continues on target, in: *Aviation Week & Space Technology*, Sept. 23, 2002, pp. 22–23.

[2] U.S. Department of the Army: *Field Manual 100-6*, 16 June 1997, originally: http://www.atsc-army.org/cgi-bin/atdl.dll/query/download/FM/100-6/fm100-6.zip. Available today at: http://fas.org/irp/doddir/army/fm100-6/index.html.

The second assertion – generating false targets by computer – is a straightforward job for electronic warfare units since the days of World War II. What then was done by dispensing aluminum foils or emitting radio signals is now being done by computer-controlled frequency emitters that automatically fine-tune the emitted signal to the characteristics of an enemy's electronic equipment. As a second point, Information Warfare comes as a modernization of electronic warfare with profound effects on warfighting capabilities.

The third assertion, having most computers in an adversaries' country go down at the start of a war, obviously is a nice thing to have in modern combat. It most of all shows the central role computers play for warfighting in any modern army. There also is a method to achieve this goal: An atomic blast test in the upper atmosphere over the South Pacific proved at the beginning of the 1960s, that the electromagnetic pulse (EMP) generated by a blast at high altitude reliably destroys most electronic equipment in a wide diameter. An atomic bomb explosion over Iraq for exactly this purpose was publicly discussed before the first Gulf War 1991[3]. Unfortunately, the EMP affects the equipment of friendly forces just as well as that of an adversary. Today, directed energy weapons are reported to be ready for battlefield use that deliver an EMP on a desired target in a small area quite similar to a ray gun in science fiction movies. As a third point, Information Warfare blurs the line between fiction and reality through skillful combination of technology proven experimentally at laboratory scale and media reports of weapons developed from these experiments.

No matter how inconsistent yet, these three hints can be used to develop a first and basic understanding of Information Warfare. The basic idea of Information Warfare is the central value of *information* – or rather data – for coordinated and purposeful military activities. Since information today is acquired, communicated and manipulated by computer, any electronic communication and computing device becomes an element for Information Warfare activities, explicitly including civilian media infrastructures. Information Warfare combines formerly separated activities in psychological and electronic warfare with the use of new opportunities generated by computer technology.

Keeping in mind that Information Warfare is not a completely new invention, we can start with the definition of Information Warfare in the terms of the U.S. Commander in Chief:

> Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks.[4]

The Army interprets its military information environment (MIE) as a part of the global information environment (GIE) and defines Information Operations (IO) in its Information Warfare Doctrine Field Manual 100-6 as:

[3] John Barry: The nuclear option: thinking the unthinkable, *Newsweek*, 14.01.91, pp. 12–13.

[4] CJCSI 3210.01, *Information Warfare Policy*, Washington 1998.

> Continuous military operations within the MIE that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; IO include interacting with the GIE and exploiting or denying an adversary's information and decision capabilities.[5]

If Information Warfare is understood as it is defined by its military proponents, there is a large number of Information Warfare methods, tools, and weapons. A press release can be just as valuable a tool in Information Warfare as a computer hack into an enemies data base. There is an even larger number of Information Warfare participants. As "significant players" in Information Warfare are seen by the U.S. Army "the media, think tanks, academic institutions, nongovernment organizations (NGOs), international agencies, and individuals with access to the information highway. [...] Their activities may cause an unanticipated or unintentional effect on military operations."[6]

When we note that information processes in this military view encompass the technological as well as the human elements of information-based processes, the global information environment – spanning the internet as well as the media and all users of these various information channels – becomes a military staging and operations area.

2 Levels of Information Warfare Reality

The scope of activities covered by Information Warfare principles is a key factor for the credibility of the concept. Influencing the media and of course psychological and electronic warfighting capabilities have for a long time been elements in modern combat. It are these elements of Information Warfare, developed and proven since more than 50 years, that make Information Warfare work on the battlefield.

Exploiting the weaknesses of information technology has become a new field of military activities with vast opportunities for destructive results. The large number of weaknesses of common computer systems – of which only a small number become evident to the general public in the form of computer viruses and the like – combined with the dependency of modern armies on computers, do not allow to ignore computer manipulations as tools in combat.

Information Warfare spans a vast array of different levels that range from non-violent and preparatory means like the ones used in psychological warfare or the exploitation of information technology weaknesses up to a massive destruction of infrastructures necessary for command and control. At the core of Information Warfare thus lies a set of *obvious capabilities* in the use of electronics, information

[5] ibid.

[6] *Field Manual 100-6*, Chapter 1.

and communication technology as well as military force and a *concept*: to achieve a maximum effect.

First of all, it is necessary to assess the use of information technology by the military. The use of computers for military purposes nowadays is most obvious in "smart" bombs or highly complex weapons systems such as warplanes that fly "by wire". Historically, so-called "mission critical" computer systems were fielded for the first time in World War II. Analog computers appeared in British air defense systems that used radar data as an input for computers that in turn controlled anti-aircraft guns. According to Wiener's memories, the computers ran his linear prediction code algorithm[7] and delivered basic ideas for Wiener's work on cybernetics.

Electronics were used to equip the most expensive and complex weapons platforms. At the end of World War II, bombers in different air forces had so-called bomb sights as electronic steering devices for the final approach on a target, while the first fighters had cathode ray tubes for target acquisition by radar on board. Since the 1950s, more and more phases of flight control, communication and targeting have been supported by "mission critical computer systems"[8]. The Vietnam war saw terrain-following bomber types like the F-111 flying at altitudes below 50 meters towards their targets where the pilots directed the plane while the onboard computers actually flew the plane and kept it from crashing into obstacles. Today, aviation computer – avionics – systems are used to keep inherently unstable airplanes in the sky[9]. The success in the use of these systems was one factor in the integration of computer systems into land-based weapons platforms as well, leading to vehicle computer systems – so-called vetronics – for tanks and others.

Modern autonomous weapons systems make an even higher demand on computer power than manned vehicles. Their development also started with the control of airborne weapons systems. An early example is the analog flight-control computer on the German V-2 rocket, which was used to steer the rocket on its exhaust plume during liftoff as on any ballistic missile of a certain size. After engine shutdown, the V-2 flew on a ballistic trajectory[10]. The first integrated circuit chips were put onto Minuteman intercontinental ballistic missiles to severely reduce their target devia-

[7] He even noted that the program made use of the fact that the pilots mostly took evasive action as recommended by their Luftwaffe drill. Wiener gives a short, but very interesting description of his work in World War II in: Norbert Wiener: *Kybernetik. Regelung und Nachrichtenübertragung im Lebewesen und in der Maschine*, Düsseldorf 1963, pp. 30ff. (German translation of *Cybernetics or Control and Communication in the Animal and the Machine*, Cambridge, Mass. 1961).

[8] See an overview in: Ingo Ruhmann: Supercomputer mit Flügeln: Avionik; in: Ute Bernhardt, Ingo Ruhmann: *Ein sauberer Tod. Informatik und Krieg*, Marburg 1991, pp. 127–153.

[9] Examples are the Swedish JAS 39 "Gripen", and the U.S. F-117A stealth fighter and B-2 flying wing bomber.

[10] Helmut Hoelzer: 50 Jahre Analogcomputer; in: Norbert Bolz, Friedrich Kittler, Christoph Tholen (Hg.): *Computer als Medium*; München 1994, pp. 69–90. For additional accuracy, improved V-2 models until engine shutdown were supported from a ground station by a guiding radio beam ("Leitstrahl" – the steered V-2 models had an antenna on one of their rocket fins, for more details see: http://www.v2rocket.com/start/deployment/leitstrahl.html).

tion – or circular error probable[11]. With the dramatic cost reductions in integrated circuits came the integration of computer processors into fire-and-forget weapons and "smart" ammunition as well as all types of weapons platforms.

Computers in autonomous weapons

The technology that has evolved into modern autonomous weapons was developed from remotely controlled systems. An early example of one of the more prominent technologies are video-controlled platforms. The first experiments on video guidance of aerial vehicles date back to World War II when German troops experimented with planes that were controlled by radio and equipped with electronic television cameras to transmit pictures to a control station on the ground. The Maverick missile in the Vietnam marked the first use of video-guided missiles in combat where an operator had to keep a target in the center of a video picture transmitted by the missile warhead. Today, computer processors aboard video-controlled systems keep a target in their aim automatically once this is locked on by an operator.

Laser-guidance technology has been developed in the U.S. since 1962. Laser-guided bombs were first used 1968 in Vietnam, their first major success came in 1972 with the destruction of a bridge. Laser-guided systems are equipped with a detector that measures the intensity of a laser reflected from a target that in turn is illuminated by a laser beam. An on-board processor generates commands for the steering system to guide the bomb or missile towards the point of maximum laser reflection. The laser illuminators and warheads can be synchronized through the pulse modulation of the laser beam. Target illumination with lasers has been done from forces on the ground. Only the Gulf War saw the use of planes able to pinpoint targets with lasers exactly enough for bombs to reach the desired goal[12]. Laser- and video-guided autonomous weapons were only made possible through the miniaturization of computer equipment.

Autonomously flying vehicles are mainly used to monitor a target area or – to a lesser extent – as weapons. The first flying weapon was the V-1 flying bomb in World War II that navigated by keeping a straight course with the help of a simple gyro compass. The target was reached when the fuel had run out. The V1-concept was further developed after the war in the U.S., where in 1960 the MACE cruise missile was demonstrated that could compare radar data with preprogrammed images and the Regulus that could fly at supersonic speed[13]. Still, both were susceptible to interception and target deviation. The modern concept of cruise missiles became operational when computers could be put on board that not only could cruise the missile at low altitude, but also could compare a three-dimensional

[11] See Holger Iburg: *Abschreckung und Software. Computertechnologie als Instrument der amerikanischen Sicherheitspolitik,* Frankfurt 1991, p. 109.

[12] See Alberto Mondini: Laser für militärische Zwecke, *Umschau* **3,** 1985, pp. 172–178; Chris Cooper: Military use of lasers, *Miltronics*, August 1983, pp. 127–131; an overview on technology and bomb types: http://www.fas.org/man/dod-101/sys/smart/lgb.htm.

[13] Die Cruise Missiles, *Österr. Militärzeitschrift*, Nr. 1, 1979.

radar map of way points and the target area against incoming signals from the on board radar to achieve a precision of just a few meters on target. The accuracy of navigation allows for cruise missiles to be used against targets in urban areas. This sensor-based kind of navigation is supported today by the GPS satellite navigation system in order to reduce the emission of radar signals.

Smaller versions of cruise missiles are called drones; these are mostly used for intelligence gathering over a confined area of a battlefield. Unmanned small reconnaissance vehicles are used by many modern armies in combat. While many armies have used drones for some time – the Israeli Scout, the Canadian-French-German CL-289, the French Brevel or the U.S. Gnat – the U.S. forces managed to draw the interest of the media with the debut of the large Predator spy drone over Bosnia operated from Hungary[14]. The Predator is now the vehicle with the longest endurance over the battlefield, which allows it to be flown from greater distances. Newer designs call for micro drones with the size of a peanut and the ability to fly over a battlefield as well as within rooms in an urban warfare setting[15]. The development today combines these developments and aims to have autonomous missiles that dispense small weapons drones[16]. One early example is the tank-breaking drone Taifun of the German Army that can fly over a target area, scan the area below for radar signatures of tanks and propel itself onto the target, when such a target is recognized[17]. Predators are currently considered as weapons-carrying platforms for the Afghan theater.

Data communication – weaving platforms and weapons into a strike package

The accuracy of weapons delivery in the Gulf War resulted not as much from the development of any single technology – be it airplanes or steering mechanisms of weapons – as from the integration of formerly singular platforms and their weapons into a digital communication system. Data sharing between platform and weapons delivery mechanism – be it a bomb or a rocket – data sharing between different platforms on and over the battlefield and data sharing between the platform and intelligence gathering units as well as auxiliary information and data distribution networks improved the effectiveness of weapons delivery systems.

[14] David A. Fulghum: Predator to make debut over Bosnia, *Aviation Week & Space Technology,* July 10, 1995, pp. 47–48.

[15] See a discussion of beginnings, cf. Bruce D. Nordwall: Micro air vehicles hold great promise, challenges, *Aviation Week & Space Technology,* April 14, 1997, pp. 67–68. U.S. Special Forces are using UAVs today, cf. Michael Dornheim, Michael A. Taverna: War on Terrorism Boosts Deployment of Mini-UAVs, *Aviation Week & Space Technology,* July 8, 2002, pp. 48–50. The French Army today has an acquisition program for such a type of UAV, cf. Michael A. Taverna: French plan for miniature UAV demonstration, procurement, *Aviation Week & Space Technology,* June 17, 2002, p. 63.

[16] David Fulghum, Robert Wall: Small UAVs built for use from large UAV's, missiles, *Aviation Week & Space Technology,* July 22, 2002, pp. 192–195.

[17] The concept for the German Bundeswehr weapon dates back from 1988, see: Kampfdrohne Heer, *Wehrtechnik*, No 5, 1990, p. 52.

A precondition for any platform to deliver any explosive device with precision is accurate navigation. Navigation of piloted and autonomous airborne systems for a long time depended on gyroscopes that had to be corrected by radar measures. A change came with the U.S. Global Positioning System (GPS), developed after experiences in the Vietnam War. GPS consists of 24 satellites in low earth orbit that emit coded signals allowing for a measurement of one's location. The first 11 satellites were put into orbit between 1978 and 1985, the last of the original configuration in 1993[18]. GPS is controlled by five military ground stations around the world and coordinated by USAF Space Command at Schriever AFB, Colorado[19]. GPS signals were divided into, (1) the military "precision" code, allowing a position fix with less than 10 meter accuracy, and (2) the deliberately less precise "coarse/acquisition" code of GPS for civilian users, which had a 100 meter accuracy. Since different technologies using ground-based signal emitters (Differential GPS) or the Russian satellite navigation system "Glonass" as a corrective to distorted GPS signals have improved the precision of the civilian signal, it was switched to military precision in 1999 through a directive of U.S. President Clinton[20] in an unsuccessful move to discourage the build-up of the European counterpart "Galileo". After U.S. Congress mandated in 1994 that all new systems must make use of GPS navigation whenever necessary, it is by now the standard navigation system for U.S. Forces, giving precise information on their respective location to manned airplanes, land and sea vehicles, autonomous vehicles, intelligent munitions as well as individual soldiers on the battlefield.

Navigation, however, plays only a small part in the activities of the kind demonstrated since the Gulf War. Since mid-World War II, bombers entering hostile aerospace are accompanied not only by fighters to engage hostile fighter planes, but also by planes with capabilities for navigation and coordination. These command and auxiliary tasks today have led to the development of a triad of command and control systems that make up the decisive factor in the effectiveness of modern air forces.

In bombing campaigns, forward air controllers selected targets and observed the effect of air strikes from small planes. The Vietnam War showed the necessity for an airborne early warning and control aircraft that could coordinate bombing campaigns for an extended period of time. U.S. Forces equipped a Hercules C-130 transport with communications and electronics to coordinate the execution of the air tasking order. The result was the Airborne Battlefield Command Control

[18] Mark Tapscott: Extending GPS on land, sea and air, *Defense Electronics*, July 1993, pp. 42–47, p. 42. The last of the first round of GPS satellites were switched off in 1997 and have been replaced by updated Block-II and Block-III satellites. Until 1997, 37 GPS satellites were launched, cf. Craig Covault: New GPS broaden navigation accuracy, *Aviation Week & Space Technology*, Jan. 20, 1997, p. 22.

[19] GPS was initially controlled by the 14th U.S. Air Fleet at Falcon Air Force Base, Colorado. The Air base was renamed to Schriever AFB in 1998, the GPS part reorganized into the 50th Space Wing's 2nd Space Operations Squadron of the USAF Space Command. See: http://www.spacecom.af.mil/hqafspc/Library/FactSheets/FactsSheets.asp?FactChoice=9.

[20] Jeanne Rubner: USA beenden Störung von Satelliten-Signalen, *Süddeutsche Zeitung*, 3.5.2000, p. 8.

Center (ABCCC) that was substantially modified in the 1990s. The massive use of computers in the system today allows an ABCCC to command and control activities in the airspace over a target area, to share data with other command posts and is capable to give commanders a so-called "God's eye View" of the battlespace[21].

Since World War II the defense of carrier battle groups against air strikes and other attacks has led to the development of airborne early warning systems that loiter in the airspace over battle groups extending the range of radar sensors against incoming aircraft and of other sensors against hostile submarines. In the outgoing 1960s, attack planes flying below the horizon of ground-based radar stations made the use of downward-looking early warning radar systems necessary for defense of land forces as well. The result in 1972 was the development of the Airborne Warning and Control System (AWACS). AWACS systems characteristically have a large rotating radar radome situated on their back to give a wide-angle view of the airspace around and below the plane. The NATO E-3 AWACS fuse the data they receive with signatures from their data base and coordinate fighters to defend an airspace. AWACS need vast computing power for sensor data fusion, communication and control in real-time and data exchange with other platforms[22].

The third leg of the airborne command and control systems triad is the E8-C Joint Surveillance Target Attack Radar Systems (JSTARS). It was also developed in the 1970s, became operational at the beginning of the 1990s and is used to detect and monitor movements of vehicles and troops on the ground in real-time over an area of an Army corps. JSTARS uses a multi-mode side looking radar to detect, track, and classify moving objects on the ground deep behind enemy lines. Radar sensor input must be interpreted by computers and is matched against signatures of known objects[23]. The on-board computers store the tracks of possible targets as they move. The data are transmitted in real-time to ground stations[24] and between JSTARS and AWACS. JSTARS were the only platform able to track down Scud rocket launchers during the Gulf War. JSTARS are improved today to attack of

[21] Myron Struck: Airborne C^2 platform proves indispensable in Gulf War, *Defense Electronics*, May 1991, pp. 22–23; Robert Wall: New ABCCC tactics used in NATO air strikes, *Aviation Week & Space Technology*, April 26, 1999, pp. 32–35.

[22] See: David A. Fulghum: Scud hunting may drop under 10-minute mark, *Aviation Week & Space Technology*, Feb. 21, 1994, p. 90. David Hughes: AWACS data fusion under evaluation, *Aviation Week & Space Technology*, March 7, 1994, pp. 49–50. wt-Telex, *Wehrtechnik* 5/93, p. 18. AWACS must not be mistaken to exist only in the kind of the configured Boeing 707 known from NATO Forces. The E-2C Hawkeye is the turboprop maritime counterpart for carrier battle groups, the Brazil and the Swedish Air Forces use Saab business jets, Russian Forces modified transports like the IL-76, see John Fricker: Russian AWACS programs face funding problems, *Aviation Week & Space Technology*, Dec. 4, 1995, pp. 89–92.

[23] JSTARS, *Soldat und Technik*, No. 9, 1997, pp. 518–522; David Hughes: Mitre, Air Force Explore Data Fusion for Joint-STARS, *Aviation Week and Space Technology*, March 7, 1994, pp. 47–48.

[24] At the beginning, the basic configuration of JSTARS consisted of one VAX 11750 to control the radar, a Litton 85A for target movement measurement, four AN/AYK-14 processors with 625 million instructions per second each for signals data processing. Control is exercised by three VAX 860. The software measures 800.000 lines of code, see John Haystead: JSTARS – real-time warning and control for surface warfare, *Defense Electronics*, July 1990, pp. 31–39, pp. 34ff.

quickly moving and maneuvering targets with the GPS-guided Joint Direct Attack Munition released from a fighter plane at high altitude. This is achieved by triangulating the position of a target from two surveillance platforms like JSTARS – or a JSTARS with a Predator drone in the near future – and transmitting the data to the free-flight bombs[25].

The "smart" bomb hitting a target thus is only the result of a computer-supported communication between intelligence platforms ranging from GPS satellites to sensor-brimming planes like JSTARS. Bombers get the data for their flight management computers and their flight route from these and other sources indicating enemy positions on the way to the target area. When the ordnance officer in the bomber identifies a target, locks the sensors of the weapon on it and releases the load, only the final step of a complex set of preprogrammed activities is executed. The taped videos of the warhead or of the ordnance control pod of the fighter, the data from JSTARS and the ABCCC are again used for the so-called battle damage assessment and to restart the cycle, if necessary.

From the air to the ground

An obvious implication of the systems described is their use for ground forces as well. GPS is a result of orientation problems in the jungles of Vietnam. The civilian mode was deliberately built into the system to develop a civilian market for small hand-held GPS receivers driving down the prices for military orders as well. JSTARS explicitly was developed to aide ground commanders in battle through real-time data on hostile troop movements. Commanders can link up to JSTARS and see the same data as the on board crew.

The integration of the battlespace in the air and on the ground was the centerpiece of reform in military doctrine and tactics in the 1980s. The so-called AirLand-Battle doctrine – formulated in U.S. Army Field Manual 100-5 – is based on experiences in the Vietnam and Jom Kippur Wars and views a battlespace not along a front line, but as a three-dimensional maneuvering area of ground and air forces reaching deep into enemy territory. Prerequisite to the AirLand-Battle doctrine is the massing up of firepower on a small area against an enemy superior in numbers but inferior in command, control communications and – most of all – intelligence. Only systems as JSTARS and computerized C^3I – explicitly described in AirLand-Battle doctrine papers – give the advantage in speed, decisiveness, and force. AirLand-Battle is the doctrine for the U.S. Army since the 1980s and was exercised in Gulf War.

The development has gone on. The use of satellite navigation and the transmission of various intelligence data today has led to infantry units that are equipped with computers for orientation, communication and weapons control. In the 1990s, the U.S. Army published an ambitious plan called Force XXI to develop

[25] David A. Fulghum: Moving targets vulnerable to radar / weapons mix, *Aviation Week & Space Technology*, Dec. 2, 2002, pp. 66–70.

the concepts for the soldier of the 21st century. To test new equipment, but most of all new tactics, the second armored division in Ft. Hood, Texas, was completely restructured and equipped with laptops, digital communication gear, and a totally interoperable C³I-system[26]. The division exercised extensively and under realistic conditions[27]. Additionally, further means for enhanced "power projection" through improved weapons and cooperation were tested, to give small units greater firepower[28]. The idea is to equip the soldiers with GPS navigation to pinpoint their own location and to transmit it to other friendly forces. A miniature video camera is used to transmit target information, a handheld computer is used to communicate maps, target and other data. In exercises at least, a higher lethality of these units was demonstrated as a result of their improved coordination and accuracy in fight. Many of the systems tested have made their way onto the battlefield. Press pictures of special operations units on the battlefields in Afghanistan sometimes show troops equipped with GPS receivers, miniature video cameras or small video visors on some of the helmets.

This has shown that military organizations depend most heavily on computers when military command is concerned. Computer-controlled sensors collect the intelligence data that are first transmitted via computer networks to military headquarters where they are combined into a coherent military status report. What is going on at what place on the battlefield or on the whole globe is the central prerequisite for any commander to make a decision. Military communication networks propagate his decision and necessary additional data to the troops on the spot, thus allowing a commander to control his troops. Through sensors and communications links, the development of the initiated military maneuver is retransmitted to the commander. These four steps of *command, control, communications* and *intelligence* – called C³I by its acronym – are the cornerstones of any purposeful military activity. The integration of all friendly military units on the battlefield into a C³I system allows a large number of military units to act in coordination and with timely precision.

It should be noted that computerized command and control has intensified the trend toward decentralized command through improved communications and the distribution of intelligence data to commanders in the field giving them an improved "situational awareness" of their tactical situation and of that of hostile troops. Since they now can call upon the support of intelligence assets and highly precise aerial strikes, the obvious result is an intensification of firepower in the first place. This, on its part, has to be matched with an improved coordination between all friendly units. The data on exchanges on a local scale that are supported by surveillance units provide input for a situational overview on higher levels of the command chain. Even in the Gulf War, video imagery from special forces in Iraq was transmitted with almost no time lapse via satellite to central

[26] See also Paul E. Menoher, Jr.: *Force XXI: Redesigning the Army Through Warfighting Experiments*, at http://www.fas.org/irp/agency/army/tradoc/usaic/mipb/1996-2/menoher1.htm

[27] Army selects experimental force, *U.S. Army News*, Dec. 6, 1994.

[28] Robert K. Ackermann: Bytes transform Army, turn service roles upside down, *Signal*, May 1994, pp. 21–24.

command posts, connecting central decision making with the "warfighters" on the front lines. It thus would be an illusion to believe that decentralized warfare also decentralizes command and control – it rather brings the formerly loosely connected local commanders into the established chain of command.

The coordination of strikes and movements of air force, tanks and infantry, that started in World War II and was made possible especially through FM communication, has since been perfected into battlefield tactics – which fail, however, if they cannot be supported by computer. As with many kinds of computer-controlled activities, integrated C^3I can lead to an improved awareness of what is going on in the so-called "theater of war", to a reduction of time to reach a decision and to transmit necessary commands to the units in the theater, and an intense use of force, when better coordination allows more friendly units to operate effectively in any given area.

Just as an example, some years ago, aerial reconnaissance of the battlefield was hindered by the time it took a plane to return to base, to develop and interpret the film and retransmit the information to the commanders in the field. Today, JSTARS deliver real-time-data of a corps-sized battlefield complete with the classification of threats to any commander with the appropriate equipment. There is no time lag between target detection, threat assessment, the issuing of strike commands and the assessment of the battle damage inflicted: The commander can view the progress of an operation in real-time just as it unfolds and develops and can modify plans according to the battle situation.

C^3I on the battlefield today stands for a massive gain in speed and fire power that can be achieved by the same number of troops, leading to the notion of computers as a "force multiplier". The idea of integrated C^3I as a "force multiplier" is based on studies dating back to the early 1970s, when the U.S. Army noted an increase in military force by a factor of 2,7 to 2,9 through the use of computerized tactical command and control systems based on the appropriate communications infrastructure[29]. In the new strategic situation of military engagements of a solitary superpower with a technological lead in information technology, this idea now is a main reason for a shift in priorities for U.S. Forces. Although warplanes and aircraft carriers still amount for the largest sums in Pentagon acquisitions, the main focus of acquisitions is now on the communications networks that distribute the increasing amount of sensor data acquired by a growing number of platforms[30].

Information Warfare as a doctrine has developed from the combination of the two basic strands of development, namely computers in weapons systems and computers for command and control. Computers in weapons systems have increased their speed and accuracy. The growth in processor-controlled weapons, sensors and platforms allowed the connection of new terminal nodes to an expanding

[29] However accurate this may be, it was used to shape opinions also in Europe, see Eberhard Munk: Organisatorische und verfahrensmäßige Aspekte der Bedarfsdeckung bei Führungsinformationssystemen; in: H. W. Hofmann, R. K. Huber, P. Molzberger: *Führungs- und Informationssysteme*, München 1982, pp. 23–46, p. 30.

[30] David A. Fulghum: Pentagon priorities shift to data and networks, *Aviation Week & Space Technology*, April 22, 2002, pp. 22–23.

computer network which in turn made possible new tactics like AirLand-Battle. Securing computer systems, communication channels and sensors of one's own units or disrupting adversaries' systems by means of electronic warfare, physical destruction in a bombardment or just efficient psychological influencing of the decision-makers make up the goals and means of Information Warfare.

For these reasons, current Information Warfare units and their infrastructure often can be traced back to their descent from different origins. The U.S. Joint Electronic Warfare Center was renamed into Joint Command and Control Warfare Center in 1994 and was given responsibility for psychological warfare, operational security, and destruction of command, control, communications and intelligence (C^3I) [31]. What began in 1953 under the name of U.S. Air Force's Special Communications Center, then mutated in the 1970s into the Air Force Electronic Warfare Center, finally became the U.S. Air Force's Information Warfare Center (AFIWC) in the 1990s[32]. The same holds for networked computer systems. The World-Wide Military Command and Control System (WWMCCS), established in 1960 and leading to the development of Internet technology, mutated since 1971 into the Prototype WWMCCS Intercomputer Network (PWIN), and then again in 1993 into the current U.S. Global Command and Control System (GCCS), which provides U.S. forces with "an enhanced common operational picture, force status, intelligence support, enemy order of battle, related facility information, and air tasking orders"[33].

If the definition of Information Warfare and the necessary operative capabilities are taken seriously, one can compare operative elements and capabilities in the U.S. and similarly developed forces in the following overview.

– *Electronic warfare*
  Since the battle of Tannenberg August 1914, where the Germans fully exploited the Russian indiscriminate use of radio communications, interception of radio transmissions as a means of intelligence gathering has proved itself very effective. The methods have been direct tapping of information, if possible, or triangulation in order to pinpoint location of enemy forces. Together with the active disruption or misleading of the adversary's use of the electromagnetic spectrum, these activities are referred to as "electronic warfare" and have become a cornerstone in warfare. The advent of computers has only changed the means employed: As already described, aluminum foils (chaff) to blind enemy radar sites were replaced by computer generated emissions that specifically match the frequency and modulation of the radar sites to be foiled, while at the same time leaving the friendly systems operational. Technically thus, it is correct to state that enemy radar sites are fooled by computer-generated false images. It is by

[31] JEWC takes on new name to fit expanded duties, *Aviation Week & Space Technology*, Oct. 10, 1994, pp. 54–55.

[32] http://www.aia.af.mil/hqaia/afiwc.

[33] According to the Assistant U.S. Secretary of Defense: http://www.c3i.osd.mil/faq/.

contrast a gross exaggeration when the media imply that this is being done by means of hacking or other forms of computer intrusion.

Any kind of use of the electromagnetic spectrum by military organizations, as well as their use of the civilian communication infrastructure, makes up electronic warfare. EW explicitly includes the physical destruction of this infrastructure. A well published example for this destructive aspect of EW are HARM rockets that, when fired by fighter planes, lock their target seeker on the emissions of an anti-aircraft radar and destruct the site on impact. Belonging in this category are also non-nuclear EMP generators that have been developed and are on the verge of being fielded as a weapons system payload[34].

Since World War II, this electronic war of many different nations, even amongst allies, has been raging on without pause on a 24 hours-basis around the whole globe.

– *Psychological warfare*

Fooling an enemy is as old as war itself. The Chinese Warlord Sun Tsu is cited with the words: "Oh heavenly art of skillfulness and surreptitiousness", through which a warrior will try to fool an enemy. Deception is used to lead enemies to false beliefs of oneself: "The smart warrior will force his will upon his enemy, but he will never let an enemy force his will upon him."[35] From the stratagems of a warlord who lived 500 b.c., this tactic has developed into a broad method of influencing an adversary as well as one's own troops in many armies. Clausewitz defines war as an act to force an enemy into fulfilling one's will[36] and devotes a chapter to the ruse of war[37]. Misleading an enemy and reading his intentions are one of the major tasks for a commander on a battlefield or in planning a strategic move.

The scientific development of psychology has broadened the scope of Psychological Warfare in the 20th century. In an Information Warfare setting, Psychological Warfare Operations, or PsyOps, have a different meaning. FM 100-6 defines them as

> Operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and, ultimately, the behavior of foreign governments, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

PsyOps are explicitly meant to "magnify the image of US technological superiority" and provide content that is to be inserted into an enemy's communications infrastructure.

[34] David A. Fulghum: U.K. developing, testing directed energy weapon, *Aviation Week & Space Technology*, July 29, 2002, pp. 26–27.

[35] Sun Tsu: *Die Kunst des Krieges*, München 2001, pp. 53f.

[36] For a detailed analysis see S. Bergstein, this volume, pp. 183–215.

[37] Carl von Clausewitz: *Vom Kriege*, Hamburg 1963, pp. 93ff.

– *Integrated C^3I-infrastructure*
Computerized command, control, and communications networks can be found in armies ranging from South Korea over Israel to the United States. The degree of integration, however, varies significantly. The German Bundeswehr, for example, still has problems with the interoperability of different generations in its army command and control system HEROS[38]. Efforts to modernize the Luftwaffe command and control system EIFEL were even abandoned[39]. The only military force with an operationally significant degree of overall integration of data communication today are the U.S. Forces that began interoperability efforts in the 1960s.

– *IT-based coupling of intelligence and warfighters*
The concepts for an integrated battlefield, developed for the AirLand-Battle doctrine in the 1980s, have been put into practice in several NATO forces. Lacking infrastructural elements for intelligence gathering such as space-based assets, the intelligence capabilities of most European forces are limited. The only force with a truly global collection and dissemination capability for various kinds of intelligence are the U.S. forces that daily collect several terabytes of data. The U.S. Army alone projects as the rate of data collected and disseminated daily by the year 2010, when a force of the size of the Gulf War expeditionary forces may be in combat, to an amount of 268 terabit; when including the data of all military units the estimates sum up to a daily rate of 570 terabits[40]. These data are to be made available to an increasing extent to troops on the battlefield, according to Information Warfare doctrine that demands better "situational awareness" through superior data on the battlefield for the soldier.

– *IT as a warfighting capability*
Computer viruses, hacking, and other remote forms of disruption of enemy command and control networks is the most speculative area of Information Warfare today – speculative because of the specific combination of real background and completely implausible assertions.
On the side of reality, intrusion into enemy computer systems dates back into the 1970s, when U.S. intelligence agencies and special forces admittedly were successful in gaining physical access[41]. Implausible is the idea that professionals responsible for communications security would take the extremely negligent step to connect a sensitive computer system to an insecure network. This risk is only

[38] See Stephan Söffing: DV-Unterstützung für die Führung des Heeres, *Wehrtechnik*, 8/94, pp. 33–37, p. 33.

[39] Hans-Josef Salm: Was lange währt..., *Wehrtechnik*, 6/92, pp. 74–76, p. 75.

[40] W. E. Howard, D.K. Evans: Growth in data speed creates opportunities and bottlenecks, *Signal*, Sept. 1994, pp. 67–68.

[41] One of the rare public statements can be found in: Jay Peterzell: Spying and sabotage by computer, *Time*, March 20, 1989, p. 41. From other sources reporting on their work on computers of western origin in the former Soviet bloc, it can be deduced that sensitive computer systems of the former Soviet Union military command were accessible to western personnel.

taken when military communications links are destroyed in war and the civilian infrastructure is the only available way to transmit the data. When one adds to this the manifold of command and control computer systems of most countries that only interconnect partially, one must cautiously differentiate between possible ways and means of attack, such as hacking into Internet computers in some other country, and fiction, when it comes to hacking the computers of a military command network.

– *Fighting by Information Warfare principles*
Many singular elements of Information Warfare doctrine are already in use; some experimental U.S. units such as the Force XXI Army unit or the U.S. Air Force's 609th Squadron already wargame by Information Warfare doctrine. Waging war completely by Information Warfare principles, however, is not in sight.

This overview on capabilities making up Information Warfare and Operations should lead to a differentiated look on Information Warfare. Many military and paramilitary organizations have capabilities and opportunities to use electronic and psychological warfare or even to hack computers. If we interpret this as Information Warfare, it would already be a fact. But: Information Warfare is not meant and defined to be just that simple. We therefore conclude that Information Warfare rests on military capabilities already well developed, and is being developed further to acquire a greater role for military forces. What we can observe is a process of gradual development of a new form of military operations into maturity.

Now that the use of computers by military organizations and their capabilities concerning different elements of Information Warfare has been elaborated, the question remains, to what extent the manipulation of computers by digital means – instead of explosives – plays a role in actual Information Warfare.

3 War by Remote Control – on Computer Network Attacks and IT Security

The media have declared Information War several times in the last years. Following the conflict between the U.S. and the People's Republic of China over a U.S. spy plane in April 2001, Chinese groups vowed revenge and began to hack into web sites hosted in the U.S[42]. The media reported on some activities and raised fears about the advent of a so-called Information World War I. Disenchantment set in when, after some days, it became clear that nothing much had happened beyond the defacement of web sites. This kind of activity is nothing new and has

[42] On the incident: http://www.cnn.com/2001/US/05/01/china.us.plane.04/. On the reactions on the internet, cf. http://www.wired.com/news/politics/0,1283,42982,00.html; http://www.heise.de/tp/deutsch/special/info/7382/1.html.

even reached such proportions that a mirror site dedicated to tracking this kind of incident declared it could no longer keep track of the numerous hacks[43].

Similar stories are nothing new. In the Gulf War, faked news was spread about computer viruses in Iraqi military computer networks inserted through a load of computer printers imported from France. In 1995, the revolt of Mexican Zapatist Groups was accompanied by e-mail battles for the mailboxes of the media between Zapatistas and the Mexican government, just like the mail battle between Peru and Ecuador accompanying their border dispute in the same year. Similar kinds of online battles have happened regularly since as a part of the conflicts in Northern Ireland, with Basque separatists and Tamil Tigers in Sri Lanka. Between Israel and the Palestinians, the so-called "inter-fadah", the Information War begun in October 2000, rages on as well as the online quarrels between the People's Republic of China and Taiwan.

These visible, but rather unsophisticated quarrels are cited as the beginning of a more dangerous kind of computer intrusion by state actors to disrupt the civilian and military infrastructure and to spread insecurity. These fears are fueled by the term "computer network attacks", defined by the U.S. Army as:

> Computer network attack consists of operations that disrupt, deny, degrade, or destroy information resident in computers and computer networks. It may also target computers and networks themselves.[44]

This definition neither distinguishes between civilian or military computer systems nor between the kind of information it aims to destroy or degrade. By this definition, any information on any computer system might be a target for a computer network attack.

Since Cyber Warfare today more often has elements of a publicity activity than as a serious security threat, the most important effort is to differentiate between the media hype, the potentials of computer network attacks and the IT security problems that worry security experts. This part will take a closer look at the players, their weapons, and the fragile IT security they exploit. The aim is to differentiate between the dangers cited, the intentions declared by cyber warfare proponents and the realities behind these assertions.

3.1 IT security still fragile

The potential for the exploitation of IT security holes and the belief of the general public in the threat posed by it is founded on the fact that IT security is rather underdeveloped. Regularly, computer viruses and Internet worms demonstrate to a broad audience the vulnerability of networked computers. It thus need not be elaborated further that severe security problems exist in IT systems opening up leaks in the security even of sensitive systems.

[43] Press statement from attrition.org at: http://www.attrition.org/news/content/01-05-21.001.html.

[44] U.S. Department of the Army: *Field Manual 3-0, Operations,* Washington, June 2001, pp. 11–19.

For two reasons, many of the real problems are only rarely discussed outside expert circles. The first reason obviously is the lack of interest of the organizations affected in discussing their IT security problem in the open. Organizations with IT security problems quietly try to fix them. Hacker attacks on companies have a high estimated number of unknown cases because police authorities are rarely contacted. The second reason is less obvious. IT security problems in computer systems usually are quite complex. The understanding of the risks and their implications often requires a deep insight into information technology. These conditions are a severe hindrance for a discussion in public media.

Real problems with IT security and manipulated computer systems thus are reported mostly in expert circles. The rare instances discussion problems in public can be found on the internet, most notably the online information service – relayed by means of a newsgroup – comp.risks. Computer emergency response teams (CERTs) and government agencies such as the German "Bundesamt für Sicherheit in der Informationstechnik" (BSI), responsible for IT security in Germany's public sector, share their knowledge with interested parties[45]. But few of even the most alarming findings are ever reported in the public media.

Surveys over the last 15 years have shown however, that most of the security problems do not result from malicious hackers but from badly designed or dysfunctional software or the incorrect handling of IT systems. Connecting badly designed or administered systems to the internet inevitably results in security leaks giving hackers access to sensitive data such as files of credit card numbers[46]. Of course, credit card numbers are not the only valuable data on the Internet, but unlike any other kind of threat assessments, there remains no doubt about the potential damage.

This should leave no doubt that IT security still has to cope with huge deficits in knowledge, consciousness, and technology. Even without malicious activities, the security situation is fragile and far from standards established in mature technologies.

3.2 Mismatch between media coverage and threats

The relation between IT security problems and media coverage always has been a quite irrational one. Periodically, reports on hackers altering web sites or breaking into Pentagon computers hit the news. A closer inspection of the cases often reveals that no real damage has been inflicted beyond unauthorized access to a system or the defacement of some web pages.

What often is seen as a serious damage will seem less so when viewed from a security perspective. From this viewpoint, a web server is a computer connected to

[45] See www.bsi.de, www.cert.dfn.de in Germany or www.cert.org for international problems.

[46] Florian Rötzer: Bisher größter Kreditkartenklau im Internet; cf. http://www.heise.de/tp/deutsch/inhalt/te/5665/1.html. Sheer neglect was the reason for accessible credit card numbers at a Berlin software company: Internet-Shop offenbart Kreditkartennummern, cf. http://www.heise.de/newsticker/data/jo-22.10.99-000/default.shtml.

the Internet for the sole purpose of providing data to web users. It should not contain any data that better should not be published. Under security considerations, web servers are considered as external resources to a company network, guarded by a firewall against outsider attacks. Because this alone cannot be considered as completely safe, the internal network of a company is additionally shielded from the company's web server by a second firewall. Attacks on web servers thus should not interfere with any sensitive activities and especially should not reveal any sensitive data.

Web servers are semi-public places that should rather be compared to the physical equivalent of an office building lobby or a building's entrance area: the guarded figurehead of a company with a high number of visitors, where no one would store sensitive data or hold sensitive meetings. In this picture, the defacement of a web page compares to a graffiti on a wall or in the lobby. It is a mark of the attacker, a nuisance for the site owner, and of course an annoyance for the company's security unit – but neither a real safety problem nor something that has to be prevented at any price. Semi-public places like company lobbies or web sites must be open to visitors and therefore cannot be completely secured. Their high symbolic value makes them an attractive goal for activities to achieve public awareness. The defacement of web sites as the electronic equivalent of graffiti is often optimized for public impact with either intelligent or outrageous content that still achieves maximum media coverage.

On the other hand, real problems with IT security have a hard time getting public attention at all. It is hardly understood by the public that IT security aims to ensure the availability, *confidentiality* and *integrity* of IT systems.

- The best-known example of severe deficiencies in the *availability* of IT systems to date has been the Y2K-bug, the inability of software to cope with the year 2000. Reprogramming old software prevented serious damage. Unchecked, this bug would have reduced the availability of computer systems to a fairly low level.
- The *confidentiality* of IT systems most often is endangered by sloppy administration or sheer neglect, as in one of the credit card examples given above where credit card data stood openly accessible in a file on the WWW-server of an e-commerce shop.
- Endangering *integrity* and *confidentiality* of IT systems is the "back orifice" software for the exploitation of security deficits in the Microsoft NT operating system. "Back orifice" is seen by critics as a trojan software and can be downloaded from the internet as freeware. It can give its users – just at the click of a mouse – total control over poorly managed NT systems online including the erasure of all data. "Back orifice" is seen as one of the most dangerous trojans freely available, but has been a lesser topic in the public media than the problems of software bugs in general. "Back Orifice" only works because of the mechanisms of software distribution on the internet. Administrators in many companies use freeware or shareware downloaded from the internet that might contain erroneously programmed or even malicious functions that may irreversibly damage the IT system of a company. But even completely refraining from using anything that is not from a big software company leads to problems when – from time to time

– some updates and patches put on the net by large software companies contain software bugs that severely endanger system integrity. The certificates used for software accuracy and authenticity do not guarantee error-free software. This at the extreme end sometimes leaves only the choice to download patches for a software bug with unknown consequences or not to download them, thereby leaving severe security holes unpatched.

Problems like these are the bread-and-butter job for IT security experts and the main risks for computer users, potentially causing the loss of data confidentiality and integrity and maybe even total system loss. The problems are real and threatening, but lack vital elements to arouse media interest. So, the most serious problems largely go unnoticed while minor troubles are willingly reported. The consequence for the public opinion is not surprising. IT security problems are seen mostly as a threat to personal data or as the spread of viruses. More complex issues are beyond the attention of the public.

Anyone trying to explain the risks and implications of computer network attacks as a tool in conflict will have to take into account the multitude of misperceptions in the general public on the relevance and the dangers associated with activities aimed at exploiting security weaknesses.

But the public debate is just one side of the coin. Many papers from security advisers and the military alike are not very helpful in bringing more insight. Dangers tend either to be somewhat exaggerated with the obvious intent to promote certain measures or remain vague in order to prevent outsiders from exploiting known bugs and security leaks. After more than a decade of papers on the feasibility of cyber warfare and little at hand to demonstrate its effects, it has become even more difficult to give a down-to-earth assessment on computer network attacks and the many other forms of cyber warfare currently being discussed.

3.3 Computers as a "weapon"

Computer networks attacks are seen as one of the dangers to IT infrastructures from a defensive point of view and as a potential means of attack from an offensive one. Beyond the level of papers and doctrines and after trying to sort out fact from fiction, the involvement in manipulations of computer networks remains elusive.

Computer systems of adversaries have been a target for intelligence and military services in the last 30 years at least. The activities concentrated on the espionage of data and the protection against it. The development of TEMPEST equipment in the late 1960s is a vivid proof. TEMPEST stands for *Tempo*rary *E*manation and *S*purious *T*ransmission and aims to prevent the transmission of data that electronic systems usually emanate, for example, when a computer terminal displays data or a printer receives data from a computer. The picture displayed on unshielded terminals can easily be received and reproduced on a TV set from a building across a street. Computer communication sent through a cable can also be inductively intercepted when the cable is physically accessible.

Emanations from unshielded electronic equipment were exploited as early as the 1950s, when British and American intelligence tapped the power cable to the cipher room of the French embassy in London. The faint signals of the electronic typewriters of the cipher machines made the original text accessible, which in turn – compared against the cipher code from these texts – compromised the crypto keys of the French system[47]. In many countries, the use of TEMPEST and the shielding of equipment became a norm in the 1960s for electronic equipment handling sensitive data. The predecessor of the German BSI – which developed from a department of the Federal Intelligence Service Bundesnachrichtendienst (BND) – TEMPEST-proved systems officially since the early 1970s.

Before the widespread use of the Internet, physical access or at least proximity to IT systems was the precondition for data gathering and system manipulation. Reports of U.S. activities date back into the 1980s[48]. Targeting computers as tools for the coordination of military activities and their communication infrastructure is the reason the Internet was built upon. Command and control of military forces has been the domain of networked computers since the early days of their development. Whirlwind – one of the first large computer projects in the early 1950s – was built to control and coordinate the status of the U.S. nuclear forces. The mainframe computers of that time were buried in hardened bunkers or mountain sites to prevent their destruction in conflict. In the 1960s, nuclear detonations were carried out in the upper atmosphere to test the effects of the electro-magnetic pulse (EMP) on electronic devices, making even sheltered systems a target as long as they were connected to a medium working like an antenna.

Since networks of computers cannot likewise be sheltered, the Internet was especially built to compensate attacks on its communication infrastructure by dispersing and rerouting data traffic around destructed network nodes. Command and control networks and their computing power have only grown in importance since. Their destruction is the prerequisite for most other military operations, making telecommunications installations, command sites and all of their respective electronic equipment and computers primary targets in any conflict.

On this level of conflict, the manipulation of computers and the use of force against installations is not at all a novel idea, but has been a military doctrine for years. Many of the activities described in modern information warfare doctrines do not go beyond the levels of data gathering on the one end of the spectrum and forcible destruction of computers and their network infrastructure on the other. If seen from this perspective, computer network attacks have been practiced for decades as a fairly lethal type of warfare. The non-lethal appearance of Information Warfare today results from the large area in between two historical poles of Information Warfare mentioned.

47 Peter Wright, Paul Greengrass: *Spy Catcher. Enthüllungen aus dem Secret Service*, Frankfurt 1989, pp. 115ff.

48 Jay Peterzell: Spying and sabotage by computer, *Time*, March 20, 1989, p. 41.

3.4 Targets for computer network attacks

Information warfare and computer network attacks as a novel approach set in on a different level. While Information Warfare concepts always stressed the need for a defense of highly IT-dependent countries against attacks on their communications and IT infrastructure, the computer network attack concept most interestingly stresses the offensive use of computer manipulations for military purposes.

Although many of the potential activities for computer network attacks hinted at in official papers will ultimately result in the same use of force as before, the idea of computer manipulations as a tool in war is not as straightforward as it might seem.

First of all, it should be remembered that security critical computers should not be networked and networked computers should not be the backbone of a critical infrastructure. Military IT systems, consequently are either connected to dedicated networks or not networked at all. How then should a U.S. military hacker enter enemy systems via the Internet when they are not connected?

The second point is the diversity of military systems. Even in NATO countries, the programming of today's military IT systems often started decades ago. Many systems are not interoperable because they work only with legacy software especially developed for solely this system. When interoperability of military IT systems is impossible between an artillery fire control system and other systems, or, for example, even between different layers of the German army's tactical Command and Control System HEROS[49], how high can the likelihood be of disrupting military IT systems with unknown source code and their interconnectivity reduced or non-existent?

The easiest way to disrupt an adversary's infrastructure is to manipulate civilian infrastructure systems, those infrastructures of the networks of communications and public utility companies, the banking system, transportation and the like. The common element of these infrastructures is their high dependency on computers and the dependency of an industrialized society on them. The proper function of these infrastructures is critical to society, which is why they are called critical infrastructures. Attacking and disrupting these computers is possible because they are interconnected to a rather high degree and are not as well guarded against attack as military systems. Critical infrastructure protection thus is a high priority in different countries.

In the U.S., the protection of critical infrastructures was assessed by a presidential commission and is a policy goal according to the Presidential Decision Directive 63 dating from May 1998. A Critical Infrastructure Protection Office (CIAO) was established[50]. In Germany, critical infrastructure protection was assessed by the "AG KRITIS" Group of BSI after a parliamentary enquiry[51] – although no

[49] As is the case for HEROS 1/2 for mobile command posts and HEROS 3 for the brigade or above; Stephan Söffing: DV-Unterstützung für die Führung des Heeres, *Wehrtechnik*, 8/94, pp. 33–37, p. 33.

[50] http://www.ciao.gov.

[51] Answer of the Federal Government to a parliamentary enquiry of rep. Dr. Manuel Kiper: *Lage der IT-Sicherheit in Deutschland*, Bt.-Drs. 13/7753, Frage 38.

results were published. Germany, however, has a more effective instrument to prevent IT security deficiencies than the U.S. since German privacy laws require organizations to follow certain security rules diminishing risks and allowing privacy institutions to check the level of safety technically implemented. The only effective measure against attacks on the critical infrastructures has basically been the establishment of new CERT groups in different countries.

The concept of computer network attacks builds on the belief that the disruption of computer systems can severely hinder any modern organization and unsettle industrialized societies. The comparison of the security precautions on civilian and military computer systems has led to the idea that it is far more effective to disrupt non-military systems, which in turn led to the establishment of organizations in several countries that – to a varying degree – try to prepare against attacks on the civilian IT infrastructure.

Since – at least until now – attacks on civilian computer networks were the acts of youthful computer enthusiasts rather than military actors, it cannot be distinguished if a computer network attack is meant as a prank of computer hacking youths or a military attack. If computer hacking in the future will be seen solely under military categories, a consequence is the extension of military thinking and military activities well into the civilian domain.

4 Political and Military Implications of Information Warfare

As we have seen until this point, Information Warfare is transforming military thinking and organizations. In most countries, this transformation process is not very structured and thorough. The activities in the U.S. military however, are far broader in scope reaching from the battlefield up to the geostrategical level.

On the *operative* level, the military doctrines for Information Warfare are refined down to the level of operative planning in the Field Manuals already referenced. The experimentation with new tools and tactics in units like Force XXI is surpassed today by the deployment of computerized special forces units on the battlefields of Afghanistan. In this conflict, and in Bosnia before, the integrated use of computers and networks for intelligence sharing and the exertion of command and control has reached a level unseen before and rather close to the concepts of Information Warfare. There still is no single integrated command network in sight, easily spanning all separate forces and the single warfighter in the whole theater of war, but the relevant data are transmitted with increasing ease between different units.

On an *organizational* level, structures for Information Warfare were already shaped in the 1990s. The Joint Chiefs of Staff installed their Joint Information Warfare Center, Air Force and Army their respective units. After first experiences with the newly set up command centers and Information Warfare units, some

restructuring has begun. Information Warfare is now the task of so many units in the U.S. forces that an overview has become confusing[52].

Even on the *strategic* level Information Warfare has become an option for a time without a bipolar world dominated by nuclear deterrence. Although the political activities to end the anti-ballistic missile treaty, ongoing since the Reagan Administration, show the unparalleled significance of nuclear weapons in political thinking, most military activities cannot rely on nuclear force, but are fought with conventional means. Since the Reagan Administration spent large sums on the development of IT-based weapons and communications systems, the advantage achieved is also used on a strategic level. The basis for the ability of the U.S. forces for a power projection rests only in part on the warplanes that can fly half around the globe or fly from bases world wide, but rather on the intelligence satellites, communications networks and precision weapons powered by computers. The ability to react with military force to achieve political goals in a short period of time has led to the notion of a "strategic army"[53] standing at the ready and being controlled from central command centers. Information Warfare in the eyes of high ranking military and political planners has become a strategic doctrine shaping alliances and operations[54].

This development is far advanced in the U.S., but has also begun in other countries as well:

- Russia concentrates on psychological and electronic warfare instead of computers[55].
- The People's Republic of China claims the concept of Information Warfare as its own idea[56] and follows similar ideas as the U.S. with an emphasis on "People's Information Warfare"[57].
- Taiwan uses the strength of its electronics industry and explores computer viruses and other means of manipulation[58].
- India is adapting ideas from the U.S. and develops similar plans for regional conflicts[59].
- In Germany, the Bundeswehr has worked on protection against Information Warfare attacks and develops Information Operations concepts for an operations planning level[60].

[52] A list dedicated to activities and actors in the U.S. forces spanning some pages can be found at: http://www.terrorism.com/infowar/j6kdefense.html.

[53] US Department of the Army: Tradoc 525-5, p. 12; http://www-tradoc.army.mil/tpubs/pams/p525-5toc.htm

[54] J. S. Nye, Jr., W. A. Owens: America's information edge, *Foreign Affairs*, March/April 1996, pp. 20–36.

[55] Igor Panarin: InfoWar und Autorität; in: G. Stocker, C. Schöpf (eds.): *Information. Macht. Krieg,* Wien 1998, pp. 105–110.

[56] Shen Weiguang: Der Informationskrieg – eine neue Herausforderung; in: G. Stocker, C. Schöpf (eds.), *Information. Macht. Krieg,* Wien 1998, pp. 67–91.

[57] Wei Jincheng: Der Volksinformationskrieg; in: G. Stocker, C. Schöpf (Hg.): *Information. Macht. Krieg,* Wien 1998, pp. 92–104.

The political and military implications of Information Warfare concepts and ideas can only be assessed when the multitude of change is taken into account. Information Warfare is by no means a singular development, but can be translated into various forms of military activities. Just as new weapons systems like tanks and airplanes or modern weapons have led to mechanized warfighting as well as guerilla warfare concepts, Information Warfare ideas will be adapted differently according to specific military strengths and weaknesses. Especially, highly asymmetrical conflicts between powerful military forces on one side and militarily very weak groups will be affected by Information Warfare.

The broad use of Information Warfare concepts and the strong effects of Information Operations against civilian targets together will lead to a new challenge in security politics.

At the basis of the problem is the temptation of attacks against civilian IT infrastructures by weak adversaries and the idea of military actors to interpret attacks on IT systems according to military terms. Although almost 700 unauthorized attempts to access Pentagon computers are recorded per day, leading to the number of 250.000 attacks published by the Pentagon in 2001, a conflict constellation on a military level is extremely rare today. A change in the nature of the mostly youthful attackers is not plausible any time soon. The interpretation of intrusions into computer systems as military attacks although would quickly and significantly change the whole picture. Hacking, which is seen under German law as a crime only when guarded systems are attacked or data are altered (a restriction which aims at keeping a naive youngster from involuntarily starting a criminal career), could immediately mutate into an act of war. Although this interpretation is proposed by no one in Germany, and even in the USA the disproportion between the deed and a military reaction is still seen clearly, the discussion in the last years has slowly developed in this direction. A clear distinction between the civilian realm of IT security and its military side of Information Warfare is clearly missing.

More important for securing IT systems is the interest of military proponents of Information Warfare in keeping weak spots of IT systems open for manipulations. The most prominent example for the diverging interests of the civilian and the military side is the use of crypto systems. Since the 1970s, U.S. intelligence agencies and the military first worked against the development of strong encryption systems[61] and, after losing the battle for control over cryptological research in the USA, the export of crypto systems and know-how.

[58] Florian Rötzer: Taiwans Militär probt Angriffe mit Computerviren, *telepolis*, 8.8.2000, http://www.heise.de/tp/deutsch/special/info/6955/1.html.

[59] C. Uday Bhaskar: Trends in warfare: a conceptual overview, *Strategic Analysis*, Dec. 2000, pp. 1577–1589. See also Ajai K. Rai: Media at war: issues and limitations, *Strategic Analysis*, Dec. 2000, pp. 1681–1694; and Vinod Anand: An integrated and joint approach towards defence intelligence, *Strategic Analysis*, Nov. 2000, pp. 397–410.

[60] Ralf Bendrath: Informationstechnologie in der Bundeswehr, *telepolis*, 25.7.2000, http://www.heise.de/tp/deutsch/special/info/6933/1.html.

[61] Explicit against the development of strong encryption was the former NSA director Admiral Bobby Inman: The NSA perspective on telecommunications protection in the nongovernmental sector, *Cryptologia*, July 1979, pp.129–135, p. 129.

Transferring this view to IT security means that the interest in Information Warfare opportunities obviously leads to an interest in IT security weaknesses, since only insecure systems are vulnerable to attack in Information Operations. Instead of securing IT systems against manipulation this policy would lead to insecure systems that most likely will be hacked by youths with plenty of time and know-how. Even harsh punishment will not keep IT systems safe and the kids from experimenting. This line of thought fueled by military interests only leads to an increasing cycle of IT insecurity where IT security weaknesses open up opportunities to so-called cyber terrorists that in turn demand decisive military activities leading to an escalation of activities with no improvement in security.

IT insecurities that lead to conflict escalation instead of more stability are the least attractive point when Information Warfare implications are concerned. Even military planners concede that it would be dangerous to make the reactions in a political crisis dependent on the development of attacks on computer systems. The different clashes on the internet between opposing parties have only shown that in a case of tension a number of individuals seem determined to show their opinion through the manipulation of other people's computers. When a defacement of web sites or even the unleashing of a computer virus can be an act of a private person in a time of tension, and since it cannot be distinguished from any organized activities, the whole concept of Information Warfare beyond its use in open military action is at best useless and at worst dangerous.

The only way to prevent such a development is a strictly non-military view on IT security, which at least seems the preferred way within Europe. When it comes to catching the author of a computer virus, a cooperation of police forces of different countries clearly is a better strategy compared to a conflict between military forces. This is all the more sensible when we look at the statistics that show that military actors have played no role so far in IT security problems.

The best ways to improve IT security would be to fund research for secure systems and to find some new mechanisms for some of the internet communications protocol features, which today are necessary elements for internet message transfer but are also used as tools in distributed denial of service attacks. If the solution would be a division into a secure and an open internet or a new set of protocol routines is open to discussion. It would also be sensible to include critical IT infrastructures in arms control agreements or other means of international cooperation that lead to international stabilization[62].

Political and technical means for stabilization are at hand also in the age of Information Warfare. The only precondition is the political will to realize the dangers of inactivity and the opportunities for the solution of the problems. It should be clear that there are possible solutions to the problem instead of the mere solutions to the symptoms as the proponents of Information Warfare favor.

[62] On the minimal steps necessary, cf. Ingo Ruhmann: Back to the Roots; in: Jörg Tauss; Johannes Kollbeck; Jan Mönikes et al. (eds.): *Deutschlands Weg in die Informationsgesellschaft*, Baden-Baden 1996, pp. 403–412, pp. 411f.

http://www.springer.com/978-3-7643-1634-1

Mathematics and War
Booß-Bavnbek, B.; Høyrup, J. (Eds.)
2003, VIII, 420 p. 79 illus., Softcover
ISBN: 978-3-7643-1634-1
A product of Birkhäuser Basel