Disruptive technologies and force transformation: A Canadian perspective

Ingar O. Moen and Robert S. Walker
Defence Research and Development Canada, 305 Rideau Street, Ottawa, Canada K1A 0K2

ABSTRACT

Transformation of Canada's military forces is being pursued to ensure their relevancy and impact in light of the new defence and security environment. This environment is characterized by an increasingly complex spectrum of military operations spanning pre- and post-conflict, the emergence of an asymmetric threat that differs substantially from the peer-on-peer threat of the Cold War, and the globalization of science and technology. Disruptive technologies – those that have a profound impact on established practice – are increasingly shaping both the civil and military sectors, with advances in one sector now regularly seeding disruptions in the other. This paper postulates the likely sources of disruptive technologies over the next 10-20 years. It then looks at how science and technology investments can contribute to force transformation either to take advantage of or mitigate the effects of these disruptions.

Keywords: disruptive technologies, force transformation, asymmetric threat, security environment

1. INTRODUCTION

By any measure, the global advancement of science and technology is at a pace never before seen in history. Disruptive technologies – those that have a profound impact on established practice – now appear with increasing frequency in both the civil and military sectors. Advances in one sector now regularly seed disruptions in the other.

A decade is now a very long time in terms of S&T advances. In the past 10 years alone, the civil sector has witnessed the birth and widespread accessibility of the World Wide Web, personal communications, digital photography, video gaming and genomics, all of which have had or are having a profound impact on military capabilities as well. In the defence sector, technology disruptions that have become commonplace in the past decade have included the introduction of Uninhabited Aerial Vehicles, precision weapons and information operations. On the other hand, technology disruptions have also emerged that have been counterproductive to society or to the capabilities of western militaries. Key examples include computer viruses, suicide bombers and the proliferation of NBC capabilities.

In parallel with this increased frequency of technology disruptions has been a growing complexity in the conflict spectrum driven by a complicated mix of social, political, religious, economic and environmental factors. The consequence has been the emergence of a new defence and security environment faced by western militaries, an environment that differs fundamentally from that experienced during the Cold War.

To ensure their relevance and effectiveness in this new context, Canada's armed forces are embarking on a path of transformation – a process of systematic reinvention of military capabilities through a combination of technological, process and organizational innovations.

This paper is organized in three parts. First, it examines trends in science and technology in both the civil and military sectors that are the likely seeds of technology disruptions over the next 10-20 years. It also discusses various considerations that may mitigate the positive influences of these disruptions in each sector. Secondly, it identifies the factors that characterize the new defence and security environment. Finally, it discusses the approach being pursued within Canada to transform its military in response to this environment, and how science and technology is being positioned to enable this transformation.

2. DISRUPTIVE TECHNOLOGIES

Defense Transformation and Network-Centric Systems, edited by Raja Suresh,
Proceedings of SPIE Vol. 5820 (SPIE, Bellingham, WA, 2005)
0277-786X/05/$15 · doi: 10.1117/12.608440

2.1 Trends

Understanding the relevance and potential impact of disruptive technologies is integral to providing state-of-the-art science and technology leadership within the defence environment. To ensure that the Canadian Forces (CF) remain technologically prepared and operationally relevant in a future defence and security environment, it is essential to be aware of the emergence of potentially disruptive technologies both for the provision of new and innovative defence capabilities or for countering any potential detrimental effects. By disruptive technologies, we mean new or existing technologies used in an innovative fashion that significantly alter established practice.

An example of a disruptive technology is that of the personal computer. The PC dramatically changed the computer industry – and the way we use computers. The initial computing performance of the PC paled compared to the mainframe computer; but the PC competed on different performance metrics (among them, size, and cost). The principles of disruption are applicable to the military as well as the private sector. The rise of the submarine and the effects it had on maritime warfare during World War I (and thereafter) bear the hallmarks of the disruptive process.

The rapid pace of technological advances provides a serious challenge to any technology-based organization – and today most organizations are technology-based. Monitoring these advances in order to determine which technologies should be pursued requires both time and money. Making investment decisions regarding which technologies to research and develop has more serious implications. The wrong technological bets can result in an organization being unable to carry out its mission – if not actually being undone.

Rapidly advancing technologies in the civil sector with potentially disruptive implications for the military sector include nanotechnology, biotechnology and biomedicine, advanced computing and information technologies and cognitive neuroscience. New developments in each of these technologies will have a significant impact on society, but the most disruptive innovations will likely occur at their intersections. The *convergence* or synergy arising from their combination is expected to lead to such capabilities as:

- Expanded human cognition and communication enabled by brain implants, new drugs, rapid learning and direct brain-to-machine interfaces.
- Improved human health and physical capabilities enabled by nano-biosensors to monitor and repair bodily functions, and systems that enhance human sensors.
- Responsive and collaborating autonomous intelligent systems to support decision-making, and nano-robots for surveillance and medical applications.

An example of a specific defence capability that could be enabled by integrating developments in nano-, info- and cognitive technologies is an integrated helmet with tunable hearing, night vision, communications, physical and auditory protection providing tactical awareness and cognition of “in-field” activity. Other examples include integrated wearable, wireless miniaturized sensors, communications and computers woven into the fabric of uniforms/body armor. Nano- and biotechnology integration has the potential of producing nano-engineered molecules or machines to detect and counter known and unknown biological, chemical and nano-weapons.

The National Science Foundation and the US Department of Commerce envisage Nano-Bio-Info-Cognitive convergence as a means toward improving work efficiency, learning, enhanced sensory-cognitive capabilities, brain-brain interactions, human-machine interfaces, and ameliorating physical or cognitive decline in humans[1].

Examples of potential technology disruptions that will increasingly be seen in military operations in the next 10 years include (each is discussed in further detail below)[2]:

- Autonomous intelligent systems and platforms
- Wide-band mobile wireless networking
- Passive Sensing for Intelligence, Surveillance and Reconnaissance (ISR)
- Micro-satellites
- Hyper-spectral sensing
- Non-Lethal Weapons (NLW)

- Micro-Electronic Mechanical Systems (MEMS)
- Power sources

Autonomous Intelligent Systems (AIS) are computer-automated systems that perform independent planning of an operation based on the high level instructions that they receive and the details of the local environmental situation provided by their sensors. Examples of roles and missions include: confuse opponents through diversionary operations; provide close reconnaissance support to manned reconnaissance operations; point vehicle in route reconnaissance; and autonomous multi-spectral, multi-agent detection and identification system for perimeter security role. In an urban scenario, AIS could simultaneously invade urban buildings with heterogeneous multi-robot teams (10's-100's) from rooftops, from ground level, and from subterranean level. In the mid- to long- term (say, from 5 to 30 years hence) we can expect to see a progressively more complex set of AIS capabilities in operation: (a) independently-acting sensing; (b) pattern recognition and adaptive learning; (c) single, independently-operating robotic platform, incorporating the capabilities of (a) and (b); (d) many interacting, sharing, cooperating and collaborating robotic platforms; and (e) human brain interacting directly and collaboratively with computer systems mounted on robotic platforms. While a number of these systems are in the very early stages of development and prototyping, all of these systems are expected to be in place by about 2025.

Wireless communications have become one of the main communication tools used by all military forces. Over the next ten to fifteen years, commercial wireless systems will allow data rates of several Mbps. In terms of data communications, this would allow complete situational awareness to be transmitted to all personnel (this is not to say that all data will be available to all personnel). The challenges include security, availability, reliability and performance.

The trend is from Active toward **passive sensing** for Intelligence, Surveillance and Reconnaissance (ISR). As the shift continues towards wireless communications (for convenience and cost-effectiveness) and network enabled systems (for performance), the occupancy of the electromagnetic (EM) spectrum will increase. The current EM spectrum is very poorly used. Policy and regulations for EM spectrum usage will eventually shift from static frequency allocation to dynamic on-demand allocation. In ten years there will be orders of magnitude more communications and active sensor transmissions to intercept. As a result, it will be possible to carry out many of the intelligence, surveillance and reconnaissance functions passively. Targets of interest include indoor and outdoor communications systems, weapons systems, air defence systems, navigation devices, transponders, etc. Passive ISR will be able to rapidly locate transmitters both indoor and outdoor with targeting accuracy, and track them using electronic fingerprints. Air defence systems that operate entirely passively are already available.

Micro-satellites having mass less than 100 kg can be active on orbit for less than $20 million and have typical lifetimes (pre 2008 estimates) of 2 years. For the next 5 years typical payloads will be small passive optical systems, small active optical systems, and passive Radio Frequency (RF) systems. In the longer term (5 to 10+ years), advances in autonomous space control will allow the inclusions of small clusters of micro-satellites to be integrated as virtual sensors for improved performance and may allow some radar applications. Optimistic projections from the Canadian Space Agency (CSA) suggest that commercially useful Synthetic Aperture Radar (SAR) systems in this domain will be feasible in the 2010 time frame. Missions of interest to the CF include surveillance of space (satellite monitoring and possible ballistic missile applications), low-resolution earth environment monitoring (hyper-spectral applications) and tracking and identification of RF emitters on the earth's surface.

Hyper-Spectral remote sensing has made huge strides in the last two decades regarding spatial and spectral resolution. There are currently sensors in space that have high spatial resolution (sub 0.5 m) as well as high spectral resolution (greater than 350 bands). These sensors are pushing terabytes of data down to earth on a daily basis. As computing power increases and new techniques are discovered in digital image analysis, we will be able to significantly increase the accuracy of surface attribute recognition. While discussing remote sensing, we must not neglect active sensors such as radar. More and more platforms are mounted with this type of equipment and the knowledge regarding radar image processing is increasing every day. Moreover the penetrating properties of radar allow us to view items that are not visible to spectral remote sensing devices

Non-Lethal Weapons (NLW) are explicitly designed and primarily employed so as to incapacitate personnel or materiel, while minimizing fatalities, permanent injury to personnel and undesired damage to property and the environment. NLW technologies include electromagnetic, chemical, acoustic, and mechanical and kinetic technologies. The mechanical and kinetic technologies (e.g., barriers, entanglements, and blunt impact) are well developed and not surprisingly, are the most commonly used in NLWs now available. NLWs based on these technologies are perhaps approaching their developmental limits from a science and technology point of view. Directed energy (i.e. electromagnetic and acoustic) and chemical (i.e. agents that affect the central nervous system or operation of equipment subject to the legal constraints) technologies, on the other hand, have greater growth potential, although whether such developments will still permit a genuine 'non-lethal' tag to be applied to weapons that incorporate such technologies is questionable.

Within the next ten years, a wide range of **Micro-Electronic Mechanical Systems (MEMS**) will be available, incorporating various sensors, actuators, transmitters and power sources on a single chip. Development of future MEMS and nanotechnology devices may ultimately rest on the ability to manufacture and package adequate power sources. The deployment and insertion of MEMS into future weapon systems and sensor networks has the potential to significantly enhance operational performance. The small weight and size of MEMS makes it possible to integrate many devices into various types of equipment. A field of distributed unattended, small MEMS-based sensors can act to co-operatively communicate for detecting and tracking of targets, border security, and environmental monitoring. Other applications include: miniature Chemical/Biological analysis instruments, hydraulic systems, propellant and combustion control, low-power/high resolution information displays, lower weight weapon systems and platforms, disaster resistant buildings, and mass data storage devices.

Power sources, from tiny batteries to megawatt diesel generators, are key to all military operations. They power field medical devices; communications; command, control, computer systems; mobile platforms; water production; camps, etc. Every soldier, weapon platform, and military mission relies on quality power. Electric power is a technology enabler and mission essential commodity. Numerous power generation technologies are being evaluated, including; fuel cell power for the 21st century, the all-electric ship, hydrogen as fuel for engines and turbines, molecular motors, boot-heel strike electrostrictive power, micro turbo generators that can be embedded into handheld devices, and chip mounted fuel catalyst, battery and thermal electric device for portable power generation and storage. These power source technologies will influence the shape, size, weight, range, and performance capability of every electrically powered device, from vital sign monitors, to command and control systems, unmanned aerial vehicles, directed energy weapons, as well as land vehicles, aircraft, naval vessels, and satellites.

2.2 Cautions

While the above trends speak to important improvements in the human condition on the one hand, or to important new military capabilities on the other, there are a number of cautionary notes that merit mention. These factors have the potential to either mitigate the potential positive benefits of these S&T advances, or to result in undesirable technology disruptions.

For example, the same advances in science and technology that are spurring societal improvements are increasingly targets for exploitation by criminal or terrorist elements. An obvious example is the emergence in recent years of identity theft enabled by the progressive digitization of commerce, now the fastest growing criminal activity in North America. Criminals are also taking full advantage of the potential of biotechnology to roll out an array of low-cost, high-potency illegal drugs, for example, the so-called club drugs and predatory drugs. The terrorist events in the US in the fall of 2001 were enabled in part through the innovative exploitation of S&T.

There is also a growing concern in the science community over the mounting evidence of a diminution in the trust that society has traditionally conferred in science. This phenomenon is not attributable to any single factor, but rather is linked to a complex combination of social trends. One dimension can be associated with high profile failures on the part of the science community to appropriately communicate or otherwise inform the public on the risks associated with S&T advances; Europe's rejection of genetically modified organisms is one such example. As another example, the general distrust that society holds for nuclear energy is resulting in the gradual elimination of this sector.

The increasing pace of technological advancement coupled with technological convergence is resulting in growing complexity, whether at the individual component level, at the systems level or at the systems-of-systems level. Our capacity to understand, design and predict the behaviors of such systems is indeed very limited and presents a potential bottleneck to the otherwise unfettered advancement of technology. There are many examples that demonstrate the problem, for example, the failure of the North American electrical grid in August of 2003. The interdependencies inherent in critical information infrastructure such as the banking system, has resulted with increasing frequency in a component or point software failure having an unpredicted and catastrophic effect on the entire system.

In the military sector, the emergence of the asymmetric threat, largely rooted in failed or failing states, is unquestionably altering the nature of conflict. The asymmetric threat challenges the power base of western militaries in two fundamental ways. First, while the asymmetric threat has very limited means to bring harm to its adversaries, it is able to apply readily available technologies to great effect. Examples include remote, wireless detonation of improvised explosive devices and suicide bombers. Secondly, the asymmetric threat typically operates from a firmly held ideological precept, therefore bringing considerable will and commitment to the conflict. A perceived vulnerability of its adversary that is regularly attacked by the asymmetric threat is the undermining of the will of the adversary's society to support the conflict.

The successful exploitation of the potentially disruptive technologies discussed above depends implicitly on the ability of the military human element to adapt. It is not necessarily obvious in many instances that this is either desirable or realistic. For example, human factors considerations may outweigh or mitigate any technological multiplier. There may also exist a fundamental lack of understanding of how to achieve the adaptation.

Finally, there is a collection of factors tied to the complexity of designing and acquiring a military capability that is at the system-of-system level. Current challenges that may mitigate the potential successful exploitation of disruptive technologies include system-of-system design and procurement, forecasting and containment of cost of ownership and achieving and maintaining operational- through technical interoperability.

3. THE NEW DEFENCE AND SECURITY ENVIRONMENT

The new defence and security environment is characterized by a number of fundamental shifts from the conditions predominant during the Cold War.

First is the emergence of an asymmetric threat that, unlike the Cold War threat, does not possess comparable military means but alternatively demonstrates great will often rooted in what would be deemed to be irrational behavior by western standards. The asymmetric threat also demonstrates the capability of being able to exploit otherwise readily available technology in innovative ways that nevertheless result in disruptive effect.

Second is the globalization of science and technology. The timeframe in which a leading-edge military technology provides operational advantage continues to shorten as either the technology proliferates or advances in other technological areas mitigate its effectiveness. The widespread access to increasingly low-cost but powerful civil-sector technologies is also the source of much of the technology disruptions that the asymmetric threat is able to exploit.

Third is the growing complexity in the spectrum of military operations. No longer is preparing for and successfully executing high-intensity conflict sufficient to ensure realization of the ultimate effect being sought. Success in stabilization and reconstruction operations, often conducted under the specter of insurgency, cannot be guaranteed based solely on the operational precepts that have produced success in high-intensity conflict. In effect, militaries are increasingly required to deliver capabilities to win the "three block war", referring metaphorically to the simultaneous conduct in close proximity of high-intensity warfare, stability operations and humanitarian operations, and typically in a complex environment such as a large urban area. Arguably, as complex as is high-intensity conflict, recent experience shows that operational complexity is likely even higher at the transition from pre-conflict to conflict and from conflict to post-conflict.

No longer is the defence and security environment one that focuses predominantly on operations outside North America. Rather the national security environment is also changing radically as the safety and security risks facing North American society expand under new health hazards, climate change, bio- and cyber- terrorism, and vulnerability of critical infrastructure. This in turn adds to the complexity of military operations, as the military's contribution to the security of the homeland becomes a key priority.

The question that the above poses is how can science and technology help reduce or otherwise manage this complexity. In essence, the forces of the 21st century need to be inherently mobile and agile. Networking, sensor integration, knowledge and understanding will be key components of achieving more effective forces. The human dimension of military capability will be characterized and shaped by the ever-changing role of the human in command, in complex operational situations and in hostile environments. It is the challenge of developing and delivering such military capabilities that must shape the nation's investment in science and technology.

4. FORCE TRANSFORMATION AND SCIENCE AND TECHNOLOGY ENABLERS

Canada's Department of National Defence defines transformation as "a departmental process of strategic re-orientation in response to anticipated or tangible change to the security environment, designed to shape a nation's armed forces to ensure their continued effectiveness and relevance." Key features of this definition are its focus on a continual process of institutional change, vice a focus on an objective defining a prescribed end-state. The fundamental building block of force transformation is military capability. DND employs Capability-Based Planning supported by Concept Development and Experimentation to manage the transformation process.

A primary role of science and technology in DND is to inform, enable and respond to force transformation. It achieves this through a variety of mechanisms including S&T outlook, operational research and analysis and technology demonstration that are intended collectively to support Capability-Based Planning and Concept Development and Experimentation.

Some examples of transformative capabilities that are currently being examined through these mechanisms are outlined below.

Joint net-enabled concepts of operations are central to the transformation of defence and security organizations in response to the new defence and security environment. The progress in information and communications technology at the summit/centre of the current technology cycle coincides with the increasing need for information superiority in joint and combined operations. Networking of systems will become the dominant factor of future military systems. Network Enabled Operations (NEOps) will greatly improve information sharing, allowing decentralized and dispersed forces to more efficiently communicate, maneuver and conduct non-contiguous operations.

The **Effects Based Operations** (EBO) concept is far broader and more ambitious. EBO are operations designed to influence the will of an adversary, one's own forces or neutrals through the coordinated application of all available capabilities, in order to achieve the desired strategic objectives. An effect is the cumulative consequences across the strategic environment of any one or more actions (or tasks) taken at any level with any instrument of Government. EBO envisage coordination of diplomatic, information, military and economic levers. Effects themselves can be physical or cognitive. This involves an understanding of friends', foes' and neutrals' perceptions. Hence, the emphasis shifts to human factors and interest in complex adaptive systems. Enabling concepts include a common information environment, integrated ISR, multi-level security, a common operating picture, and operational net assessment.

Full spectrum protection against threats will remain a goal over the next decade. Limited full spectrum protection sensors will probably be achieved within the 2025 time frame. The development of armor and camouflage will depend heavily on new materials research. New fibers (e.g. spider silk produced by DNA modified organisms or nano-tube fiber systems) as well as polymeric and ceramic multi-impact resistant materials will be developed. For camouflage and armor, active systems will be developed. The soldier's suit and the vehicle covering will exhibit chameleon-like properties across the Electro-Optical (EO) spectrum.

The first level of **protection against Nuclear, Biological, Chemical (NBC) threats** will be long-range remote agent detection and identification as well as accurate propagation prediction models. Reactive neutralizing materials and self-decontaminating surfaces on military platforms will offer the second level of protection. If all else fails, comprehensive personal archival devices will help medical personnel to accurately identify exposure and treatment.

There will be increased emphasis on **footprint reduction** to reduce the demand for items, and to enhance the 'potency' of the commodities such that more value is provided per volume or mass. Emerging materials will provide many technological solutions to reduce operational sustainment with reduced footprint. New protective clothing as well as equipment components, coatings and lubricants can reduce maintenance, transportation and power requirements. Such materials provide logistics and operational benefits of longer shelf life and better performance in extremes of heat, cold and humidity. Durability and effectiveness can be improved in tandem to reduce wear-out, lengthen operational lifetimes and lower sustainment requirements in the field. Other innovations include embedded sensors and bar-coded materiel to improve ammunition and spares management in the same way that commercial checkout counters automatically re-order stock for items that are being purchased or drawn down – allowing the CF to adopt "just in time" re-supply options.

As the science and technology investment undergoes further examination for its relevance to force transformation, it is expected that increased emphasis will be placed on the science underpinning the understanding of people dimensions and future concepts, with less emphasis on the technology needs *per se* of equipment capabilities. More specifically, a particular focus will be placed on the science related to societal influences, human behavior, cognitive performance, complex systems and threat prediction.

5. SUMMARY

The defence and security environment has changed radically in the recent past, in part shaped by technology disruptions. The asymmetric threat has indeed become the conventional threat. Militaries must transform to maintain relevance and effectiveness in this new reality. Likewise, the investment in science and technology must be tailored to inform, enable and respond to the force transformation process.

REFERENCES

1 M.C. Roco and W.S. Bainbridge editors, *Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive*, NSF/DOC-sponsored report, Arlington, June 2002.

2 N. Porter, J. Kennedy, B. Bridgewater et al., Transformation *Concepts and Technologies, DRDCTiger Team Analysis of Transformation Implications*, Defence R&D Canada Technical Report TR 2004-003, April 2004.