

## MODERN TECHNOLOGY REVOLUTION FOR SECURITY

Pavel NECAS, Miroslav KELEMEN

The Armed Forces Academy of General Milan Rastislav Štefánik, Demänová 393,  
031 01 Liptovský Mikuláš, Slovak Republic, e-mail: [miroslav.kelemen@aos.sk](mailto:miroslav.kelemen@aos.sk)

### Summary

The global dimension of future security threats is of paramount importance. Whilst technological advancements will continue to be the basis of wealth for many nations, terrorism is likely to continue to be the harbinger of a pervasive sense of insecurity amongst populations. Increasingly, energy security will be the driver of many key strategic decisions, creating dynamic and unstable inter-state interactions in the process. With the international system itself experiencing a period of profound flux, some of the institutions that are charged with managing global problems may be overwhelmed. The likelihood of great power conflict escalating into total war is lower than at any time in the past century but weak governments, lagging economies, mass migration, WMD proliferation, religious extremism, and youth bulges, will align to generate the conditions for internal regional conflicts with global impact, backed by the Revolution in Military Affairs.

Keywords: Technology and Military Transformation, Security technology, Research and Development, Risk-Threat-Vulnerability, Life-time cycle, Afghanistan, National strategies, Emerging technology, Energy Security, Innovative approach, Revolution in Military Affairs

### 1. INTRODUCTION

Globalization and the spread of information technology will combine to put increasing strain on the concept of state, but will not alter the geographical dimension that remains a key parameter. After due consideration of the levers impacting the future strategic environment, together an analysis of the trends of key factors such as resources, economies and populations, the resultant is likely to be a scenario of states linked by common interests, cultures, expectations and ambitions, that rotate around pivotal states acting as regional attractors. An additional level of complexity arises due to the dynamic interaction between the geographical and virtual dimensions possibly inducing centrifugal forces as individual nations cluster around pivotal states.

Technology has a range of implications for national governments: the impact that scientific and technological developments have on society, the economy and the environment; what the latest trends are; what the future might hold; and how this all affects security, both internal and external. Therefore, science and technology, research and development considerations, and others have to be included in the factors determining national strategy.

Technology has offered a high and sophisticated standard of living to societies but at the same time introduced an inherent vulnerability. Without its tools their economies can no longer be run and their infrastructure would collapse. Modern societies and their armed forces have become highly dependent on modern technology. The

unarmed attacks of 9/11 clearly demonstrated this and the public is generally not aware of even larger threats, some at a nation's scale, posed by terrorists but also by accidents or natural disasters, just because of the total reliance on technology. Regarding military affairs, the Gulf Wars, the Kosovo air campaign and the war against terrorism in Afghanistan sharpened the public's interest in the military applications of high technology, through television pictures of the precision use of smart weapons and stand-off weapons platforms. The myth of the "zero-loss war" was actually born in Kosovo. Immediately deriving from this experience, the reluctance for casualties and collateral damage would have grown and influenced to some extent the political attitude of Governments in taking part into operations, eventually being able to influence up to the nation's strategy.

### 2. GEO-STRATEGIC ANALYSIS

The strategic repercussions brought about by the end of the Cold War are still unfolding: emerging powers in Asia, retrenchment in Eurasia and a roiling Middle East. The very magnitude and speed of change resulting from a globalizing world will be a defining feature of the world into the 21st century. Other significant characteristics include: new challenges to governance and a more pervasive sense of insecurity due to terrorism. As one maps the future, prospects for increasing global prosperity and the limited likelihood of great power conflicts provide an overall favorable environment for coping with what are otherwise daunting

challenges. Globalization, that is growing economic inter-connectedness reflected in expanded information flow, shared technology, interactive capital investment, inter-dependent markets for goods and services, and an increasingly mobile workforce throughout the world, will be an overarching mega-trend, capable of substantially influencing all parallel global forces.

### 3. GLOBAL DIMENSION OF CHALLENGES

An expanding global economy will increase demand for many finite raw materials e.g. oil, that is expected to become significantly scarce by the middle of the 21st century. Total global energy consumption is likely to rise by about 50 percent in the next two decades compared to a 34 percent expansion from 1980-2000. Most experts assess that, with substantial investment in new capacity, overall energy supplies will be sufficient to meet these increasing global demands. However, on the supply side, many of the areas, the Caspian/Barents Seas, Venezuela, and West Africa, that are being relied upon to provide increased output are accompanied by substantial political or economic risk. Traditional suppliers in the Middle East are also increasingly unstable. Thus sharper demand-driven competition for resources, perhaps accompanied by a major disruption of oil supplies, are among key uncertainties. Increasingly, energy security will be one of the critical elements of the security environment into the future.

Part of the pressure on governance will come from new forms of identity politics centered on religious convictions. In particular, political Islam will continue to have a significant global impact, rallying disparate ethnic and national groups and perhaps even creating an authority that transcends national boundaries. Democratization and greater pluralism could gain ground in key Middle Eastern countries that thus far have been excluded from the process by repressive regimes. Yet, the process already started in many states of the former Soviet Union and in Southeast Asia, may well prove less effective than hoped with a return to less democratic regime structures possible.

Regionally based institutions will be particularly challenged to meet the complex transnational threats posed by terrorism, organized crime and the proliferation of Weapons of Mass Destruction (WMD). Such post-World War II creations as the UN and the international financial institutions risk sliding into obsolescence unless they adjust to the profound changes taking place in the global system, including the rise of new powers (regional hegemonies). A sense of insecurity will characterize public opinion based on psychological perceptions being viewed as physical threats. Even as most of the world gets richer, globalization will profoundly shake up the status quo. This generates

enormous economic, cultural, and consequential political convulsions.

Current nuclear weapons states will continue to improve the survivability of their deterrent forces and almost certainly will find methods to better the reliability, accuracy, and lethality of delivery systems as well as develop capabilities to penetrate missile defenses. The active demonstration of nuclear capabilities by any state would further discredit the current nonproliferation regime, cause a possible shift in the balance of power, and increase the risk of conflicts escalating into nuclear ones. Countries without nuclear weapons, especially in the Middle East and Northeast Asia, might decide to seek them as it becomes clear that their neighbors and regional rivals are doing so. Moreover, the assistance of proliferators will reduce the time required for additional countries to develop nuclear weapons.

Information technology, allowing for instant connectivity, communication, and learning, will enable the terrorist threat to become increasingly decentralized, thus evolving into an eclectic array of groups, cells and individuals that do not need a stationary headquarters to plan and carry out their operations. Training materials, targeting guidance, weapons know-how, and fund-raising will all become virtually online.

Terrorist attacks will continue to primarily employ conventional weapons, incorporating new twists and constantly adapting to counterterrorist efforts. Terrorists probably will be most original, not in the technologies or weapons they use, but rather in their operational concepts i.e. the scope, design and support arrangements for their attacks. Strong terrorist interest in acquiring chemical, radiological, biological, and nuclear weapons increases the risk of a major terrorist attack involving WMDs. The greatest concern is that terrorists might acquire biological agents or, less likely, a nuclear device, either of which has the capacity to generate indiscriminate casualties on a huge scale. Bio-terrorism appears particularly suited to the smaller, better-informed groups. The terrorists will attempt cyber attacks to disrupt critical information networks and, even more likely, cause physical damage to information systems.

Mass migration will continue and, as a consequence of the low educational standards of most migrants, this phenomenon will continue to give rise to high levels of unemployment bringing with it the potential to generate ethnic and religious tensions. The resultant is the creation of a frustrated and disenfranchised human resource 'pool' with recruitment potential for terrorism.

The difficulty for national security mechanisms is then to identify such terrorists within the state boundary and uncover the 'enemy in one's own land'. And this is vital in order to prevent terrorist activities taking place that, in turn, generate

indiscriminate victims (sometimes on a large scale but not always) within the population, instill a pervasive fear amongst populations in the process and adversely impact economic systems.

Organized crime embraces the elements of money laundering, human trafficking, smuggling, drug trafficking and corruption. Together, these elements have the potential to undermine state structures and influence the power monopoly of states.

As all developed states are dependent, and becoming increasingly dependent, on Information Technology (IT) the potential impact of cyber crime, especially as a tool of terrorism, is very likely to attain a new level of importance into the future. Already only a slight interference of these complex systems can generate damage of immense magnitude.

A large number of physical disasters are forecast, in particular, as a consequence of the melting of the polar ice caps. If this materializes widespread flooding of coastal regions will follow, necessitating migration. In addition an environmental reshaping of this magnitude is likely to be accompanied by dramatic changes to weather patterns such that an increasing number and frequency of tornados, tsunamis and storms follow. The implementation of strategies designed to counter such occurrences will demand huge national and international commitment, especially in budgetary terms and, inevitably this will divert resources from other areas, including security. The security challenge presented therefore will be to continue to provide a secure environment with diminishing resources in an increasingly natural resource scarce environment. Responsibility to counter the security challenges posed falls to the respective national security organisms, in particular intelligence services and police authorities. However, the real challenge in confronting the cause of the security risks lies hidden within democracy itself as diverting huge sums of money to environmental issues lessens the amount available for health, education, welfare. Importantly, in tandem with fractured stability issues arising within member states of NATO military capability gaps will emerge and widen as individual nations divert resources from defense to other areas as other, more pressing, difficulties arise.

#### **4. GLOBAL VERSUS GEOGRAPHICAL APPROACH**

Globalization and Revolution in Military Affairs will place enormous additional strain on governments. Growing connectivity will be accompanied by the proliferation of virtual communities of interest, complicating the ability of states to govern. The Internet, in particular, will

spur the creation of even more global movements that may emerge as robust forces in international affairs.

One can rightfully ask if, in an era of globalization and 'cyberization', whether geography continues and, will continue to be a dominant value. Globalization consists largely of two aspects, one being the rise of trans-national economic actors, sometimes more powerful than states, and the other the geographical disconnection of otherwise linked economic activities, mainly between the production of goods and associated services. The 'cyberization' of communications has largely promoted the latter.

Economic activities, as they bind people and establish societies, constitute the baseline of inter-human relations. These activities are dependent on the availability of, or access to, resources (human and material) that are unevenly distributed around the globe. Geography determines the spatial pattern or distribution of these resources, be it human through living space and conditions or material through availability or, even more important, accessibility by presenting natural barriers as the mountains and deserts or natural highways like waterways and sea lanes. Of course, available technology and capital may create infrastructure that modifies these geographical features, thus influencing accessibility, but large-scale geographic barriers can rarely be completely annihilated. Geo-strategy "is not geographic determinism, but it is based on the assumption that geography defines limits and opportunities in international politics: states can realize their geopolitical opportunities or become the victims of their geopolitical situation" [4]. Even a cyber based economy will require specific human resources and infrastructure, most of the time only available in areas where other economic activities are developed.

Common economical activities shape societies and inter-societal economical exchanges are accompanied by cultural exchanges, promoting common understanding and mutual influence, the depth of which is largely dependant on the relative power balance. As geography determines spatial trade flows, it will equally influence cultural "commonality" and determine society groupings. The economical activities of a society provide the basis for its power. To determine the power distribution amongst states or regions and their evolution in the near future, it is necessary to study the building blocks constituting their power. As previously articulated, the prime power elements (or factors) constitute populations, resources in their quantitative and qualitative aspects providing a qualified labor force, availability of material resources, the capability to develop and use technology, determine the ability to change physical and human environments or to adapt to a changing environment and finally, economies in

their own right, providing capital, the ultimate means of exchange in order to acquire the resources or technology needed.

Geo-strategy is then necessarily a dynamic approach. It reflects the global constellation of power elements "arising from the interaction of geography on the one hand and technology and economic development on the other. Technology and the infusion of capital can modify, though not negate, the strategic importance of a particular geographic space".

Man-made cyber geography, the ultimate expression of globalization, is likely to exist alongside, or on top of, natural geographic features and is expected to become another example of technology modifying or reducing the influence of the natural landscape, but not reducing it to a level of inconsequential impact because that is not possible.

## 5. TECHNOLOGICAL DEVELOPMENT COUNTS!

A pertinent question is whether technological developments might bring Allies to the limits of interoperability. Over the last two decades the USA have been spending more money on developing technology than all the European partners spend together. One can argue that this kind of "gap" has always existed. The present problem could lie in the vanishing solidarity as the common enemy has faded away. Weaker Allies would have been backed up to avoid a breakthrough while now military and political authorities will rather question the opportunity of taking supplementary risks just for the "pleasure" of enjoying their company in the planned operations. A real technological gap may cause a shift in the threshold of interests for common action and could induce a political gap that would be much more damageable for NATO's cohesion.

The global information infrastructure enables any group, if not individuals, to have access to techniques for "home made" weaponry. Another aspect is the power acquired by major multinational armament manufacturers on governments as they detain the key technology to base military power on. On the other hand, some companies will only survive as long as public money is made available for Research and Development (R&D) and sometimes even just for running. Will modern technology become too expensive for some national defense industries in

a competitive and shrinking defense market?

Additionally, the fast development of technology could have in some nations an internal aspect as it is not sure that all top managers of the armed forces and their political masters are well aware of what is going on. This remark is not made to blame them but to stress that the technical complexity is now so high that it has become very

difficult for specialists to inform thoroughly and clearly the decision makers about the possibilities but also the consequences of every technical progress. This is the open door to a lot of deleterious lobbying and potentially dangerous strategic orientations and operational choices.

## 6. HIGH-TECH IMPACT: IRAQ CASE STUDY

Along with the aspect of information and media, the aspect of globalization that is affecting asymmetric capabilities of our potential adversaries is that of information technology advances. Technology was once the weapon of the strong as the US with the NATO Allies demonstrated with its overwhelming defeat of the numerically superior Iraqi Army during Operation Desert Storm.

The first night of the Gulf War air campaign demonstrated that the conduct of war had changed. Well before dawn on 17 January 1991, Major Greg Biscone flew the first of two B- 52s toward Wadi Al Kirr airfield, a recently completed forward fighter base in central Iraq.

His targets were the taxiways between the runway and hardened aircraft shelters. Skimming 300 feet over the desert at 500 miles an hour it was so dark the night vision goggles and low light TV system didn't help. Iraqi early warning radars forced Biscone to drop his huge, old bomber lower, the surface-to-air missile (SAM) threat was greater than the danger of flying within a wingspan of the ground. Minutes later, Biscone and his counterparts executed a successful multi-axis attack crippling the airfield and leaving anti-aircraft artillery with nothing to fire at but the receding jet noise. Less than an hour earlier, stealthy F-117s had struck the heart of the enemy, Baghdad, in the opening minutes of the war. Tomahawk Land Attack Missiles (TLAMs) followed, striking critical electric systems and government decision-making and communications centers. F-15Es, part of an initial covert entry scheme into Iraq, attacked known SCUD launch facilities that threatened Israel and coalition nations.

Simultaneously, 13 F-117s flew against 22 separate targets including command bunkers north of Baghdad, communications exchanges in Baghdad, interceptor operations centers in Kuwait, satellite downlink facilities and vital communications nodes around the country. In western Iraq 30 aircraft attacked Saddam Hussein's chemical production facilities. Just north of Basrah, 38 fighters put Shaibah airfield out of commission and 44 others stripped away the medium altitude SAM defenses west of Baghdad near Al Taqqadum airfield, the Habanniyh oil storage area and three chemical weapons precursor facilities to clear the way for attacks the following afternoon. All suspected biological weapons storage sites were



targeted and critical oil storage facilities were hit. Conventional air launched cruise missiles (CALCMs) fired by B-52s flying from the United States reached electric facilities at Al Mawsil in Northern Iraq. By the end of the first 24 hours of the war, bombs also hit enemy bridges, military support and production factories, and naval facilities. In all, more than 1,300 offensive air sorties were flown that day. However, it was not the number of sorties that made this first day of air attacks so important, but how they were planned and co-coordinated to achieve specific effects; this represents one of the first examples of the effective implementation of the latest modern military technology assets available.

The superior defeat in less than 100 hours had forever changed the ability of modern, technologically advanced nations to wage war. The debate still spread out about whether there was or not a Revolution in Military Affairs (RMA), but what is increasingly clear is that the technology that enabled the Allies to defeat Iraq is now becoming universally available.

Technology transfer has really taken three forms. First there is almost universal access to space-based imagery, the global positioning network, and worldwide secure communications network. Second, it is now extremely easy to purchase technologically advanced weapons such as Global Positioning System (GPS), jammers, radio direction finding equipment, night vision devices and handheld radios at a fraction of the cost had paid to develop them. Finally, the cost of modern weapons has become so great, that it has increased the dependence on joint military and civilian ventures where technology transfer to the civilian community is increasingly difficult to control.

## **7. CONCLUSIONS AND RECOMMENDATIONS**

During a fifteen minutes search on the Internet one is able to obtain high quality imagery of Washington D.C., Brussels, Pentagon, several of important nuclear facilities and almost any NATO Allies military installations. This information is available to anyone with a computer and a modem. If one is willing to pay, the information can be sent worldwide in near real time. If an adversary were planning an attack against whatever Center of Gravity (COG) as for example nuclear plant may be, this would provide an invaluable planning tool.

Access to GPS systems, satellite phones, and secure Internet communications have given criminal and terrorist networks access to the same level of information that was once available to only the most sophisticated nations. Terrorist groups and extremist organizations are making unprecedented use of this new technology as outlined in a report

by the US National Infrastructure Protection Center. "Extremist groups are increasingly adopting the power of modern communications technology. An extremist organization, whose members get guidance from

e-mails or by visiting a secure web site, can operate in a coordinated fashion without its members ever having to meet face to face with other members of the organization" [5]. First, the Internet is being used to incorporate new members into terrorist/extremist organizations and bomb them with a steady stream of propaganda. This propaganda indoctrination can be conducted from a safe area where the leaders are free from any threat of law enforcement. Secondly, access to online communication sources like free email accounts, chat rooms, and web-based bulletin boards, make it difficult to track where messages are coming from or going to. It provides a means for almost worldwide secure communication. The emergence of more sophisticated technology, like anonymous remailers, encryption and decryption, will only make identification and tracking more difficult.

And finally, Internet gathering points allow dispersed members to share ideological and operational information, enabling them to centralize their shared world view into independently actuated agendas in support of a common goal. Another reality of the globally connected world is the merging of defense and commercial technologies on a global scale. It is only logical that as our defense industries shrink and consolidate, they will have to produce products that have both military and civilian, dual use capabilities to survive. The ability to achieve competence in civilian production and defense industrial applications is becoming increasingly intertwined. At the same time, market access in the developing world (as in East Asia) increasingly requires technology sharing as an instrument of commercial competition [1].

The proliferation of weapons technology will be an increasing problem. "Technology diffusion to those few states with a motivation to arm and the economic resources to do so will accelerate as weapons and militarily relevant technologies are moved rapidly and routinely across national borders in response to increasingly commercial rather than security calculations. For such militarily related technologies as the Global Positioning System, satellite imagery, and communications, technological superiority will be difficult to maintain for very long" [2].

The greatest revolutions in military affairs are possibly more in the nature of war than in technological revolution in weapons systems, command and control devices and so on. A State is supposed to offer protection to its citizens. As for many countries the external aggressor has practically disappeared, they started concentrating

on the internal security. But the threat to internal security often comes from outside, which means that one has to go global and address the causes of the disease where they are, rather than symptoms at home. This has reoriented security policies towards more diplomacy, more co-operation and, as military forces are concerned, towards capacities of expeditionary type. This is, at least for the majority of the European Allies, such a profound change in their nature and their doctrine, their structure and their equipment that even the term "revolution" was used. NATO's success during the cold war era is undisputed. Nevertheless, after the fall of the Berlin Wall, the Alliance struggled to survive. In the security environment that follows the Balkans crisis, the concept of Collective Security emerged, thus providing grounds for the creation of an operational concept of expeditionary capability. The tragic events of the 9/11 once again forced the Alliance into new scenarios characterized more and more by a global effect of challenges. Terrorism is more identifiable as capable of diffusing a pervasive sense of insecurity rather than defining a clear and identifiable threat, nevertheless, its global reach and effect is evident. Technological advancements, energy security issues, mass migration, proliferation of WMD, internal difficulties of international organizations with the simultaneous appearance of internal conflict in states characterized by weak governance, all serves to create a global security environment of instability.

## REFERENCES

1. Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, CSIA Studies in International Security No. 4, 1994, p. 47.
2. Global Trends 2015: *A Dialogue About the Future With Nongovernmental Experts*, National Intelligence Council, NIC 2002-02, December 2000, p. 31.
3. KELEMEN M., SZABO S., SOUŠEK R.: *The development of the Slovak air forces air transport capabilities for joint logistics support operations*. In: Acta Avionica, 2006, vol. 8, number 12, pp. 114-117. ISSN 1335-9479.
4. Mackubin Thomas Owens, In Defense of Classical Geopolitics, Naval War College Review, vol. 52, no. 4 (Autumn 1999), <http://www.nwc.navy.mil/press/review/1999/autumn/art3-a99.htm>.
5. National Infrastructure Protection Center, Highlights 10-01, November 10, 2001, p. 2. 5 Ibid.
6. NEČAS P., SZABO S., BUČKA P.: *Crisis management and security in simulation environment*. In: Science & Military, 2006, vol. 1, number 1, pp. 33-37. ISSN 1336-8885.
7. OLEJNÍK F., NEČAS P.: *Challenges of the 21st century Global security: Reflected reforms*. Košice, Air Force Academy of General M. R. Stefanik in Kosice, 2004, 214 p. ISBN 80-7166-051-5.
8. SEDLÁK V., MESÁROŠ M., LOŠONCZI P., JAMNICKÝ O.: *GALILEO – nový globálny družicový navigačný systém a jeho perspektívy pre bezpečnosť ľudského potenciálu*. In: Security Magazin, červenec/srpen 2008, s. 23-27. ISSN 1210-8723.
9. SEDLÁK V., LOŠONCZI P., PODLESNÁ I.: *Družicové navigačné systémy*. Vysokoškolské skriptá, VŠBM Košice (vyd.), Košice, 2009, 75 s. ISBN: 978-80-89282-31-9.