IAI Research Papers

Istituto Affari Internazionali

Technological Innovation and Defence: The Forza NEC Program in the Euro-Atlantic Framework

edited by
Alessandro Marrone, Michele Nones
and Alessandro R. Ungaro

Edizioni Nuova Cultura

Series Editor
Natalino Ronzitti

Acknowledgements
The research team would like to thank the Italian Army General Staff, particularly the Land Transformation Department, as well as Finmeccanica-Selex ES. The authors bear the entire and exclusive responsibility for the content of this study. This research has been carried out with the support of Finmeccanica-Selex ES. Chapter 3 was translated with the support of Finmeccanica-Selex ES.

Contributors
Nick Brown, IHS Jane's International Defence Review
Tommaso De Zan, Junior Researcher, Istituto Affari Internazionali (IAI)
Maren Leed, Senior Adviser, Center for Strategic and International Studies (CSIS)
Alessandro Marrone, Senior Researcher, Istituto Affari Internazionali (IAI)
Michele Nones, Head of the Security and Defence Program, Istituto Affari Internazionali (IAI)
Alessandro R. Ungaro, Researcher, Istituto Affari Internazionali (IAI)

First published 2016 by Edizioni Nuova Cultura

For Istituto Affari Internazionali (IAI)
Via Angelo Brunetti 9 - I-00186 Roma
www.iai.it

ISBN: 9788868126513
Cover: by Luca Mozzicarelli
Graphic Composition: by Luca Mozzicarelli

Table of Contents

Executive Summary

Technological innovation and military environment have always been constantly interacting. Since the end of Cold War, this important interaction has experienced a significant increase. In this context, this Research Paper mainly focuses on the relationship between the Information Communication Technology (ICT) and the Italian, US, French, British and German armed forces. Within the euro-Atlantic sphere, it has the aim to analyse the path to the development of Network Enabled Capabilities (NEC) through the Forza NEC program undertaken by the Italian Army in the past decade. The acronym NEC refers to the interconnection of different elements of armed forces in one single network, with the aim to obtain their interaction in order to reach a strategic supremacy. This process can be achieved throughout a suitable architecture of Communication, Command, Control and Computer (C4), and the digitization of armed forces' equipment, so that it can be connected to the network.

The Research Paper is structured in three chapters, respectively giving an analysis on the US case study, an overview of the developments in France, Germany and Great Britain and finally a close examination on the Italian situation. Four years after the publication of IAI Research Paper "The Transformation of Armed Forces: The Forza NEC Program," this volume aims at focusing on the relation between technological innovation and the developments in the defence sector. The developments and efforts to digitize and interconnect the armed forces' equipment through the ICT face both operative and budgetary problems. These realities complicate the path toward the development of netcentric capabilities of the armed forces here taken into consideration.

***

In the US, ICT and NEC have become deeply and irrevocably ingrained in US military operations. The debates now are centred on how they can be best employed, not whether they should be. Networks (wired and wireless, space-based and terrestrial) play a crucial role in each of the "warfighting functions" found in US joint doctrine – Command and Control (C2), Intelligence, Fires, Movement and manoeuvre, Protection and Sustainment. There are dozens of programs, both joint and at the individual military service level, that are intended to provide capabilities in one or more of these functional areas.

As ICT have developed and created the promise of NEC, they have presented both opportunity and challenge. The opportunity lies in greatly enhanced capability not just within platforms, but across them. One of the challenges is injecting that potential across a staggeringly large inventory of equipment.

Each of the four military services is taking the same basic approach to finding the right balance between budgets and capability enhancements. Funding for new programs is being cut back significantly, but any "new starts" will be designed to be net-enabled, and with open architectures to allow for capability upgrades as ICT continue to advance. Existing equipment is being incrementally upgraded, in some cases to provide sufficient support (especially power) to allow for greater networking among disparate systems and in some cases to insert updated capabilities directly.

The Air Force and Navy are largely attempting to "pure fleet" their major weapon systems – e.g., to reduce the number of different models of ships or airplanes and achieve equivalent capabilities across them. The Marine Corps and Army, who typically have very large equipment inventories, must in many cases out of necessity have like-model platforms with differing levels of capability, creating interoperability challenges within their own units for larger scale operations. The intent is to minimize such differences to the greatest possible extent, but fiscal realities have forced the Army in particular to move to more explicit strategy of incremental upgrades across multiple programs, with differing increments across the force. Overall, however, the Army's desire to evolve from "stand alone systems to networked systems" is shared by the entire US military, and all of the services are moving in that direction.

That said, the US military recognizes that on the one hand stand-alone capabilities lack synergy, but on the other that networked ones present opportunities for adversaries to achieve much greater effects should they be able to penetrate or deny access to those networks. Evidence of these concerns can be found in the major investments the US military is making in cyber defences, though those fears are not preventing the full adoption of NEC.

In many ways, broad-based recognition of the potential ICT offered for the US military began with Global Positioning System (GPS) satellite navigation system and the positioning, navigation and timing (PNT) information it provides. PNT data have revolutionized every warfighting function, from Blue Force Tracker systems that allow commanders to “see” the positions of each vehicle in their unit in real time to the passing of precise coordinates to munitions to the use of unmanned aerial systems to deliver supplies directly to remote stations in the mountains of Afghanistan. As alluded to above, the revolutionary impact of PNT data on US military operations comes with some risk, however, and not only from cyber attacks. Increasingly, US military leaders have cautioned that space is becoming more and more congested, and also more contested. This poses a significant threat (purposeful or otherwise) to every aspect of US military operations, from communications to intelligence to the provision of logistic support.

While PNT information has been revolutionary in many ways, US military requirements for NEC now extend much further.

For the Army, the past decade-plus of combat operations have convinced all of its senior leaders that the ability to see themselves and the enemy, and to rapidly push that information around the battlefield, are crucial, and that all of this rests on robust networks. The Marine Corps, which draws most heavily on support from the other services, also recognizes that NEC offer vastly increased capability within its own formations, and are central to its interactions with the rest of the joint force. Thus while ICT specifics continue to rapidly evolve, there is consensus across the US military that its future success rests on the continued ability to better leverage those advances with NEC.

Every major program has embedded NEC. Some programs are explicitly designed to provide networks, while others indirectly leverage NEC to enhance their overall performance.

ICT and NEC are clearly here to stay for the US military, and many feel that their potential is only partially realized. However, obstacles remain. These include technical issues, still elusive interoperability, funding constraints, institutional barriers, and legal and policy issues.

a) Technology. Despite the dizzying pace of technological advancement, technical issues with NEC persist. Perhaps the most critical are those imposed by the basic physics of size, weight, and power, which continue to limit the full exploitation of NEC both for weapon systems and at the level of the individual service member.

b) Interoperability. While interoperability – with other US services as well as with international partners – is in part a technical issue, it is also a policy one. Thus interoperability continues to be a priority at multiple levels: within each military service, across the services, and with international partners. While the rhetoric is strong, however, implementation continues to lag behind. Budget pressures appear to be encouraging each of the services to "start at home," placing first priority on enhancing interoperability internally, then with the other US services, and lastly multi-nationally. Each is trying to preserve its participation in international exercises to the greatest possible extent (for both military and diplomatic reasons), which will likely continue to be the main venue for working through international interoperability issues in the coming years. With respect to acquisition policy, the Defence Department stipulates that equipment will be interoperable in general, and specifically that equipment purchased for individual operations be interoperable with all coalition partners. However, aligning investments and standards across nations continues to be a challenge. As one US Army official in Europe recently lamented, NATO countries are still unable to field radios capable of direct communications, in part because alliance interoperability does not play a sufficiently prominent role in national acquisition decisions.

c) Institutional. One of the key themes in the latest round of the acquisition reform debate is the need for the Defence Department to embrace a more nuanced, less "one-size-fits-all" approach to buying different kinds of military capabilities. In the NEC context specifically, some have suggested that the traditional acquisition system might be suitable for fixed networks, for example, but that a faster, less rigid system is needed for other ICT and related services. Others argue that the current system is viable if implemented differently. For example, some research centres have published guides aimed at helping Pentagon buyers to improve their agile acquisition practices. Acknowledging these challenges, senior Defence officials have adopted the latter approach, pledging to better utilize existing processes rather than reinvent them. To that end, the Joint Staff recently modified the official acquisition system to create a new category for information technology programs, allowing greater delegation of decision authorities.

Intellectual property (IP) rights are another key sticking point. The Defence Department has been increasingly vocal about its intent to move away from buying systems with proprietary hard- and software interfaces, a desire reinforced by the Congress. However, companies that have business models structured around long-held IP are loathe to move to more open architectures, particularly when they perceive that time is on their side. Companies that have developed key parts of major systems that are aging and need replacements or upgrades have to decide whether they want to continue to compete to play a possibly lesser role going forward.

d) Conceptual. As is discussed above, the services, and the Defence Department more broadly, all recognize the twin opportunities and vulnerabilities associated with high levels of network reliance. However, at present there is no clear consensus about how best to address the vulnerabilities. The natural predilection of the military services has been to defend, especially in the cyber arena – to increase spending on cyber defence forces, network infrastructure and design, and other key defence approaches. In space, that approach has given way to a more balanced focus on increasing both defence and resilience, for individual payloads and satellites and across constellations. In the broader electro-magnetic spectrum context, the strong focus on defence is to some degree augmented by a (culturally weaker) strain of offense borne out of the electronic warfare tradition.

e) Legal/policy issues. Finally, as is frequently the case, ICT developments in many instances move faster than do the policies and legal structures that would enable their full employment. The specific challenges associated with interoperability have been discussed above, but the problems extend to other areas as well. For example, in a US-specific context, policies governing the military services' use of cloud technologies reflect some of the tensions between security concerns, affordability, and interoperability. Ultimately, DoD decided upon a decentralized approach that allows each to independently buy digital cloud systems if those systems comply with common standards.

Another area in which technological advances are eclipsing the existing legal structure is with respect to military activities in the electromagnetic spectrum. As new capabilities are developed, many seek to integrate intelligence information with the ability to deliver effects. This possibility creates an inherent tension between Title 50 of US Code, which governs intelligence activities, with Title 10, which governs military operations. Electronic warfare has been conducted under Title 10 authorities, but the ability to marry electronic warfare activities that seek to disrupt signals with cyber operations that might seek to affect the information within those signals, for example, presents new legal challenges that have not yet been fully examined, let alone resolved.

In sum, US ground forces and their sister services are and will continue to be fully reliant on NEC, in every warfighting function and in every warfighting domain: air, land, maritime, space and cyber. The degree to which NEC is used for offensive and defensive purposes varies in each domain and function, as does the balance between a defensive versus dispersed approach to mitigating associated vulnerabilities. And while ICT and NEC have changed the way Americans do and will fight wars (and all other military missions), multiple obstacles to leveraging them still further remain. Nevertheless, the ICT/NEC bell has been rung; the challenge for the US Army and Marine Corps will be to maximize its benefit while minimizing its risks.

***

In the Old Continent, the starting point and the ambitions in the field of netcentric capabilities are partially different. France, Germany and United Kingdom have undertaken their own path for the netcentric transformation of their respective armed forces, which has been influenced also by the experience in the international missions of the last fifteen years.

For example, France's early adoption and commitment to its FELIN digital soldier ensemble and its relatively late deployment into Afghanistan enabled the country to develop a cohesive package of systems that worked together at an individual level and provided the building blocks to expand that to wider platforms on the battlefield. By comparison, the UK's similar FIST aspirations provided some initial successes, but the country's adoption of Urgent Operational Requirements (UORs) – acquisitions of systems such as radios, electro-optical sights and other systems off-the-shelf from a range of suppliers to get them into soldiers' hands as soon as possible – may in retrospect have imposed unintended limitations that eventually derailed FIST and other projects. By definition, this reactionary acquisitions process prevented the MoD from acquiring or developing elements and modules that would work together as a cohesive system. Germany's experience with its IdZ ensemble is somewhere between the two, having stuck to its original plans and concept in principle unlike the UK, but being more flexible than France and not being afraid to junk the elements that didn't work as hoped for and looking for workarounds.

As regards the threat to the network, the cyber-security gained ever more importance within the British and French conception. Both the armed forces are developing capabilities not only of cyber defence but also of attack, as compensation for the identified vulnerability linked to the digitization process of the respective armed forces. This commitment is followed by a certain activism of defence industry in the two countries. Germany has also moved in this direction, even after the recent crisis in Ukraine, in particular for what concerns the capabilities of early warning and interdiction towards cyber-attacks.

In term of C2, the British case of the architecture of communication at a tactical level Bowman is a good example of the difficulty for the armed forces at keeping up with the technological innovation in the ICT field. The Bowman system started to work in 2008 after a long gestation phase because of the complexity to digitize and network the Army's assets, and since 2015 a more updated version is being introduced. Yet already in 2018 is foreseen the substitution of the Bowman system with a new one, also known as Morpheus, which should be more easily updating in the time to keep up with the ICT developments. In France, the program SCORPION uses a centralized approach to the acquisition of vehicles, weapon and communication systems in order to obtain netcentric capabilities. Although, the upgrade of the current communication architecture, the SICS, is simultaneously financed to maintain operative the vehicles that will not be reconfigured within the SCORPION. The merge of the two programs aims to balance the need of keeping up with the ICT together with the impossibility of replacing tout court the asset legacy of French Army. Even Germany had to face similar problems. The digitization program IdZ of the single soldier's equipment – the equivalent of French FELIN – started in 2004 but it saw the delivery of the first stock only in 2012. The fact that the vehicles of the German Army are new or in phase of acquisition is a positive factor due to the fact that these are already designed to satisfy the netcentric requirements.

Generally, a more cautious approach has been adopted in all the three countries if compared to the United States. This happened also because of the budget limits and/or of the short-term needs linked to the ongoing operations. Nevertheless, they recognized the importance of the netcentric capabilities, in particular of the cyber field, investing huge economic resources in facing the difficulties generated by netcentric transformation in terms of asset legacy, interoperability and obsolescence of acquired systems.

***

The third chapter provides an overview of Forza NEC, the procurement program led by the Italian Army (IA) and started in 2007, which aims to develop a netcentric architecture with the goal to provide "information superiority" through the digitization of the armed forces. By adopting a very focused approach, Forza NEC intends to meet the operational needs of the Army acquiring specific assets and/or modernizing those already owned. In fact, the program has undertaken a significant stage of development and experimentation – the so-called "Concept Development & Experimentation" (CD&E) phase, which is the current phase of the program – to validate technological solutions in the light of operational requirements set by the Army, even through a continuous dialogue between the armed forces and the industry.

Since the end of the Cold War, the Italian armed forces have conducted missions different from the mere protection of the territorial integrity of the State. In the last two decades, the Army has deployed on average 9,000 units in international missions and 4,000 in domestic operations, with peaks of 19,000 soldiers simultaneously located in domestic and international theatres. In terms of quantity, and compared to the Air Force and the Navy, the AI is the most deployed armed force, providing approximately 75% of the total Italian soldiers in operational theatre. In 2014, the Army has deployed its soldiers in 2 national operations and in 12 international missions, totalling 10,361 units in theatre.

If one has to generalize in a nutshell what have been, and currently are, the main needs of the Army, last years' missions and operations have shown that, in the future, it would be desirable to: develop a C2 architecture able to collect and share information to effectively support the decision-making process in a timely manner; expand the ability of real-time updates of the ground situation through sophisticated intelligence capabilities; and, ultimately, strengthen all new platforms with active and passive protection systems.

In the future, the Army will continue to have a key role in supporting Italian defence policy, especially given the deterioration of the security regional context Italy belongs to. It seems more likely, however, that in the future the Army will be deployed in situations similar to those envisaged by the third strategic option, that is in international missions whose operational environment will be similar to the ones where the armed force has operated in the past 25 years. Indeed, in areas located in the immediate proximity of Italy – North Africa and sub-Saharan Africa, Middle East, Eastern Europe, the Balkans and the Caucasus – non fully democratic countries or "frozen conflicts," features of new or recurring internal wars, are still present. This option seems even more likely than the protection of the Atlantic area if one takes a look at Libya's current state of affairs.

Italy firstly revealed its interest in the netcentric capability in the 2005 Chief of the Defence Staff Strategic Concept. Considering also the rapid evolution of armies' modernization plans in other NATO countries, the Forza NEC study program was launched in January 2007 as an inter-force program led by the Italian Army. The digitization of the armed forces is the first step towards the realization of a netcentric system, that is the integration of tools and technologies into a C4I system to collect, exchange, correlate and use all the information obtained in the various stages of an operation. The collection of information permits to acquire a Shared Situational Awareness, that is the "knowledge of the operational status of forces." By the means of a Shared Situational Awareness it is possible to gain the so-called "Information Superiority," which represents a force multiplier and a key element in achieving success, particularly in the context of joint and international operations.

Forza NEC acts as a catalyst for other procurement programs, providing both updates to other current programs or influencing the technical specifications of those not yet started. Forza NEC can be considered more than a mere procurement program because its outcomes will affect the broader modernization of the Italian Army. As an evidence of this, Forza NEC subsumes other programs like SIACCON, SICCONA, BFSA and the Future Soldier.

Initially, the program was supposed to be completed in 25 years, from 2007 to 2031. However, the very nature of the financing, matched with a series of technical challenges, have significantly influenced the development and implementation of the program.

The objective of the CD&E is to produce a complete NEC architecture on a smaller and, through a series of tests, carefully evaluate the technological systems that will underpin the digitization of the Army. In other words, the CD&E seeks to produce the needed capabilities to "test and validate the architecture of the digitized force through the creation of all the main elements forming the NEC architecture on a small scale."

Nevertheless, the very nature of the CD&E – a concept development and experimentation phase – has raised a few technical and administrative problems that have produced some delays, which, however, were expected by both the MoD and the industry. For this reason, the CD&E is now set to end by 2020, instead of 2013 as previously contemplated. On the other hand, however, the CD&E phase has had two positive effects: the relationship established between the industry and the MoD and the identification of an initial set of systems/platforms/tools ready to be produced. In 2006, the total cost of the Forza NEC program was estimated by the industry at around 22 billion euros. This estimate was merely tentative as it was made before the CD&E phase itself. To date, the total cost of the Forza NEC program amounts to 815 million euros, including 15 million for the PD phase and about 800 million for CD&E phase.

The Forza NEC program presents many challenges that, if positively faced, can turn into opportunities to be exploited in future procurements programs. Among these challenges/opportunities the main are:

1. CD&E production of systems/platforms/tools;
2. Armed forces education and training;
3. Legacy assets;
4. Joint interoperability;
5. Tactical data management;
6. Cyber defence.

The production of CD&E's systems/platforms/tools represents the real question mark of the program. The limited resources available to the MoD hinders any long-term planning ready-to-use systems, platforms and tools production. Despite this, from an operational but also financial and industrial point of view, the benefits to follow up with an industrialization plan are evident. The digitization process is a challenge for the whole Army organization because it fundamentally alters the way soldiers are educated and trained. The NEC capability allows obtaining information that needs rapid decision-making and critical thinking to be exploited. Because of that, military education and training should teach how to handle large amounts of information and to manage stressful situations in which soldiers face psychological and moral dilemmas. Training will need to realistically reproduce mission scenarios/events and prepare soldiers to cope with complex future threats, also considering the possibility to be deployed in theatres different from Afghanistan. With this respect, the land training system SIAT (Sistema Integrato di Addestramento Terrestre) can ensure, together with the ITB, to adequately train the IA to the use of the netcentric capabilities.

Some challenges of the Forza NEC program stem from "structural" elements of the program itself, such as its extended duration and the technological complexity of the digitization process. As a matter of fact, to make the assets and systems of the IA netcentric, it was decided to upgrade to netcentric "standards" some of the vehicles and systems currently available, the so-called "legacy assets," while waiting for their replacement with new assets already designed according to the netcentric philosophy. As a result, during the Forza NEC CD&E phase, the Italian Army will own either updated systems, that will be replaced at the end of their operational life, or new systems with netcentric technologies already included. The potential obsolescence of new systems and platforms created and tested during the CD&E is a potential source of concern because of the speed at which systems and tools recently produced will be no longer "new" due to technological innovations. To avoid this problem, during the testing and prototyping phases, systems and platforms should be configured according to an "open architecture," seconding rapid ICT technological developments.

An additional technical challenge is to guarantee interoperability among the Italian armed forces at the end of the Army digitization process. In other terms, platforms and assets employed by the Army, the Navy and the Air Force must be able to communicate and interact with each other and also with those of other countries. For this reason, the design and development of the netcentric architecture has envisaged specific components to support interoperability among national and international armed forces.

The ability to connect a fair amount of nodes and make them communicate with each other is another important issue to be addressed, since the program aims to connect thousands of components. Forza NEC is fairly ambitious if one considers that the Navy and the Air Force, besides having started a digitization process earlier than the Army, have to connect at most few hundreds ships or aircrafts. In fact, the Navy's fleets have already been connected with each other via data link for a long time, while the Air Force already conducts operations fully using the Link–16 system for data exchange, in compliance with NATO standards. In other terms, the Army faces two problems: first, the Army starts from a lower level of digitization than the other two Armed Forces; second, it must connect an bigger number of elements in a network. Once having solved this challenge, another issue is to process the huge amount of data originating from the nodes of the network. At this moment, the netcentric system foresees the presence of intermediate nodes that should be able to filter relevant information and send it to the higher levels (Regiment and Brigade) of the command chain. This is however a temporary solution. Software are being tested to "smartly" process data from the ground, meaning to collect information only from critical nodes, and thus avoid flooding the chain of command with irrelevant information.

The Forza NEC program has been developed in a context strongly influenced by ICT developments. If the goal of the program is to achieve Information Superiority, a related issue pertains to the fact that collected data could be intercepted or the network tampered by enemies. Indeed, in a system with thousands of sensors, each "node" can represent an element of vulnerability. Against this backdrop, the "information security engineering" approach seeks to make systems more robust and resilient against possible cyber attacks. Security is further enhanced with "security hardening" activities, following assessment of information security systems conditions in the theatre of operations. Moreover, some innovative technological components such as the MILS (Multiple Independent Levels of Security) Gateway, have been designed to manage information between different domains depending on data level of classification.

In the light of the current policy that has repeatedly asserted the need to "do more with less," the modernization of the land component becomes crucial. Investments in technology would allow to replace assets worn out by operations, to better manage resources and to protect soldiers in theatre. Consequently, what is now a reality – a close collaboration between the industry and defence sectors working side by side from the beginning of a program – will hopefully be consolidated in the future and allow Italian armed forces to be in line with the innovation of other foreign armed forces, keeping costs on a sustainable track and with the perspective of sharing efforts with the EU and NATO.

***

Lastly, in the light of the analysis included in the three chapters, the conclusions take into account the impacts of the ICT revolution. Furthermore, they evaluate if, how and how much the Italian armed forces and those of the main NATO members considered in the Research paper are able to take advantage of the opportunities offered by the ICT and to manage the risks connected to it. The main assumption is that technology is not and cannot become the solution to all security dilemmas, given the fact that the future operative environment will still be characterized by human dimension, which will still be part of every conflict. If it is true that technology itself is not sufficient to achieve military objectives of a country such as Italy, it is also true that it is absolutely necessary – a real condition sine qua non. In particular, today and in the near future the netcentric transformation of the military capabilities represents an undeniable transition in order to maintain the efficiency and the validity of the armed forces.

List of Abbreviations

4G LTE	4th Generation Long-Term Evolution
A2/AD	Anti-Access, Area Denial
ACV	Amphibious Combat Vehicle
AEHF	Advanced Extremely High Frequency
AFATDS	Advanced Field Artillery Tactical Data System
ALAT	Aviation Légère de l'Armée de Terre
AMPV	Armoured Multi-Purpose Vehicle
AOC	Army Operating Concept
BatCIS	Battlefield Tactical Communications and Information System
BCIP	Bowman and ComBAT and Information and Platform
BFSA	Blue Force Situational Awareness
BIGSTAF	Breitbandiges, Integriertes GefechtsSTAnd Fernmeldenetz
BISA	Battlefield Information System Application
BIT	Brigata Integrata Terrestre
BMI	Bundesministerium des Innern
BND	Bundesnachrichtendienst
BTID	Battlefield Target Identification Device
C2	Command and Control
C2I	Command, Control, Intelligence
C2N	Command Control and Navigation
C2PC	Command and Control Personal Computer
C3	Command, Control and Communication
C4	Communication, Command, Control and Computer
C4I	Command, Control, Communications, Computers and Intelligence
CAC2S	Common Aviation Command and Control System
CALID	Centre d'analyses en lutte informatique defensive
CANES	Consolidated Afloat Networks and Enterprise Services

CD&E	Concept Development & Experimentation
CDR	Critical Design Review
CEC	Cooperative Engagement Capability
CEMA	Cyber Electromagnetic Activities
CEMP	Capacité d'Engagement Multi Plates-Formes
CeSiVa	Centro di Simulazione e Valutazione dell'Esercito
CEWCC	Cyber and Electronic Warfare Coordination Cell
CFI	Connected Force Initiative
CIA	Capabilities Integration Assessment
CID	Combat IDentification
CIS	Communication and Information System
CMF	Cyber Mission Force
COMCEPT	COMplément de Capacités en Elongation, Projection et Théâtre
CONTACT	Communications Numériques TACtiques et de Théâtre
COP	Common Operational Picture
CP	Command Post
DARPA	Defence Advanced Research Projects Agency
DCGS	Defence Common Ground System
DCPP	Defence Cyber Protection Partnership
DEM	Data Exchange Mechanism
DGA	Délégation Générale pour l'Armement
DII-LD	Defence Information Infrastructure - Land Deployable
DoD	Department of Defence
DSB	Defence Science Board
DVB-RCS	Digital Video Broadcasting-Return Channel Satellite
DVB-S2	Digital Video Broadcasting-Satellite Second Generation
EBRC	Engin Blindé de Reconnaissance et de Combat
EDA	European Defence Agency
EF	Expeditionary Force
EHF	Extremely High Frequency
EMARSS	Enhanced Medium Altitude Reconnaissance and Surveillance System
EMP	Electromagnetic Pulse
EMS	Electromagnetic Spectrum

ESA	European Space Agency
ESCPC	European Satellite Communication Procurement Cell
FAC	Forward Air Controller
FCS	Future Combat System
FELIN	Fantassin à Équipement et Liaisons Intégrés
FIS-H	Führungsinformationssystem Heer
FIST	Future Infantry Soldier Technology
FMN	Federated Mission Network
G/ATOR	Ground/Air Task Oriented Radar
GBA	Generic Base Architecture
GCCS	Global Command Support System
GCHQ	Government Communications Headquarters
GIS	Geographic Information System
GPS	Global Positioning System
GrATS	Ground Asset Tracking System
GSA	Generic Soldier Architecture
GTIA	Groupements Tactiques Interarmes
GTWLFD	Gateway of the Digitized Landing Force
GVA	Generic Vehicle Architecture
HCDR	High Capacity Data Radio
HeATS	Helicopter Asset Tracking System
HF	High Frequency
HMT	Helicopter Mission Trainer
HQ	Headquarter
IA	Italian Army
ICC	Integrated Command and Control
ICT	Information Communication Technology
IdZ	Infanterist der Zukunft
IdZ-BS	Infanterist der Zukunft Basissystem
IdZ-ES	Infanterist der Zukunft Erweitertes System
IED	Improvised Explosive Device
IFV	Infantry Fighting Vehicle
IoE	Internet of Everything
IP	Intellectual Property

IP	Internet Protocol
IPv	Internet Protocol version
ISAF	International Security Assistance Force
IT	Information Technology
ITB	Integration Test Bed
JBC-P	Joint Battle Command-Platform
JC HQ	Joint Command Headquarter
JIE	Joint Information Environment
JLTV	Joint Light Tactical Vehicle
JPADS	Joint Precision Air Drop System
JRD	Joint Regional Detachment
JSF	Joint Strike Fighter
JSTARS	Joint Surveillance and Target Attack Radar System
JTRS	Joint Tactical Radio System
JUICE	Joint Users Interoperability Coalition Exercise
KFOR	Kosovo Force
LEAPP	Land Environment Air Picture Provision
LE TacCIS	Land Environment Tactical Communications and Information System
LFD	Landing Force Digitalizzata (Digitized Landing Force)
LMV	Light Multirole Vehicle
LOSA	Land Open Systems Architecture
LRS-B	Long-Range Strike Bomber
M&S	Modelling and Simulation
MAST	Maritime/Air Systems & Technologies
MBT	Main Battle Tank
MCCIS	Maritime Command and Control Information System
MILS	Multiple Independent Levels of Security
MIP	Multilateral Interoperability Program
MIP-DEM	Multilateral Interoperability Program Data Exchange Mechanism
MiSE	Ministry of Economic Development
MLRS	Multiple Launch Rocket System
MMTV	Multirole Medium Tactical Vehicle
MND-SE	Multinational Division South-East

MoD	Ministry of Defence
MRAP	Mine-Resistant, Ambush-Protected
MSU	Multinational Specialized Unit
NATO	North Atlantic Treaty Organization
NCIRC	NATO Computer Incident Response Capability
NCW	Network Centric Warfare
NEC	Network Enabled Capabilities
NG	Next Generation
NIE	Network Integration Evaluation
NTM-A	NATO Training Mission-Afghanistan
OSCE	Organization for Security and Cooperation in Europe
PD	Project Definition
PFI	Private Finance Initiative
PIM	Paladin Integrated Management
PNT	Positioning, Navigation and Timing
PRR	Personal Role Radio
R&D	Research and Development
RAF	Royal Air Force
RAP	Recognised Air Picture
RFID	Radio-frequency IDentification
RIFAN	Réseau IP de la Force AeroNavale
RITA	Réseau Intégré des Transmissions Automatiques
RMP	Recognised Maritime Picture
ROI	Return on Investments
RPAS	Remotely Piloted Aircraft System
RSTA	Reconnaissance Surveillance and Target Acquisition
SAIM	Système d’Aide à l’Interprétation Multi-capteurs
SATCOM	Satellite Communication
SBIRS	Space-Based Infrared System
SCA	Software Communications Architecture
SCORPION	Synergie du COntact Renforcé par la Polyvalence et I’InfovalorisatiON
SDR	Software Defined Radio
SDSR	Strategic Defence and Security Review

SEGREDIFESA/DNA	Secretariat General of Defence/National Armaments Directorate
SHF	Super High Frequency
SIACCON	Sistema Automatizzato di Comando e Controllo (Automated Command and Control System)
SIAT	Sistema Integrato di Addestramento Terrestre
SICCONA	Sistema di Comando, Controllo e Navigazione (Command, Control and Navigation System)
SICF	Système d’Information pour le Commandement des Forces
SICRAL	Sistema Italiano per Comunicazioni Riservate e ALlarmi
SICS	Système d’Information et de Combat SCORPION
SIR	Système d’Information Régimentaire
SIT-ALAT	Système d’Information Terminal de l’ALAT
SitComDé	Système d’Information Terminal-Combattant Débarqué
SMD	Stato Maggiore della Difesa (Defence General Staff)
SOF	Special Operations Force
SOP	Standing Operating Procedure
SOTM	SATCOM On-The-Move
STANAG	Standardization Agreement
SVFFuA	Streitkräftegemeinsame Verbundfähige Funkgeräteausstattung
TAAC-W	Train Advise Assist Command-West
TCN	Tactical Communications Networking
TENCAP	Tactical Exploitation of National Capabilities
TRADOC	Training and Doctrine Command
TSMPF	Tenue de Situation Multi Plates-Formes
TTP	Tactic, Technique and Procedure
UAV	Unmanned Air Vehicle
UGV	Unmanned Ground Vehicle
UHF	Ultra High Frequency
UK	United Kingdom
UN	United Nations
UNIFIL	UN Interim Force in Lebanon
UOR	Urgent Operational Requirement
US	United States
VBM	Veicolo Blindato Medio

VBMR	Véhicule Blindé Multi Rôle
VCC	Veicolo da combattimento corazzato (Armoured fighting vehicle)
VMF	Variable Message Format
WGS	Wideband Global SATCOM
WIN-T	Warfighter Information Network-Tactical

1.

US Ground Forces and Network Enabled Capabilities: Finding the Balance

Maren Leed

1.1 The state of the art of the American debate

One could argue that the US defence establishment has a somewhat schizophrenic relationship with the idea of network-centric warfare. Land forces proponents in particular have historically resisted the conception that advances in Information and Communication Technology (ICT) have resulted or will bring about a "revolution in military affairs." However, ICT in many ways underpins the key tenets of US military concepts and force design, especially as the US defence budget falls. At the strategic level, the debate is essentially one over whether ICT presents circumstances that fundamentally alter the nature of warfare itself. At the operational level – that is, in the areas of concepts, doctrine, and procurement – there is much greater consensus that ICT offers significant capabilities that are increasingly central to future US military activities.

At the same time that the Network Enabled Capabilities (NEC) derived from ICT advances are becoming so fundamental to the US military's future, there is broad recognition that networks also present crucial vulnerabilities. There is a very strong emphasis on cyber defence in particular, and evidence of continued tensions between the desire to exploit all of the opportunities NEC offer and the fear that such dependence carries with it the seeds of eventual defeat.[1] In the words of one

[1] See, for example, US Dept of Defence, *Quadrennial Defense Review 2014*, March 2014,

Defence Department official, the US "has spent hundreds of billions of dollars" working communications and intelligence, surveillance and reconnaissance "and weapon systems that no one can match [...] But the problem with those systems is that [...] as great as they are, they are as vulnerable as the networks that connect them."[2] Recognition of the imperative to defend networks has been strong for years, and a variety of approaches are being taken to mitigate the inherent vulnerabilities associated with US forces' network reliance. Efforts to exploit NECs' offensive potential are less well coordinated, but at the highest levels the US is fully committed to leveraging ITC and NEC as integral to future military operations.

This consensus strengthened as the wars in Iraq and Afghanistan progressed. Though the fielding of NEC in each was uneven, the demands of both conflicts accelerated their employment or advancement in multiple areas. Prior to the onset of Operation Enduring Freedom in Afghanistan, the interest in NEC was more narrow, and tended to focus primarily on wired networks. The parallel paths of rapid commercial development and full engagement in complex, asymmetric campaigns have fundamentally altered the ICT/NEC conversation for the US military. The services as a whole are now broadly focused on leveraging both wired and wireless networks, and on understanding the implications of those activities in the context of operations within the electromagnetic spectrum (EMS) more expansively. ICT and NEC have become deeply and irrevocably ingrained in US military operations; the debates now are centred on how they can be best employed, not whether they should be.

This chapter provides a brief overview of some of the primary steps that US ground forces in particular are taking to advance the employment of NEC in each of the six warfighting functions found in US joint doctrine. These functions are intended to reflect the major elements that would require consideration when developing any military plan or activity in

http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf; US Dept of Defence, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, January 2012, http://www.defense.gov/news/Defense_Strategic_Guidance.pdf.

[2] Jordana Mishory, "Official: DoD needs to better coordinate, oversee electronic warfare efforts", in *InsideDefense.com*, 15 October 2014.

order to ensure a comprehensive and integrated whole. While each of the US military services uses slightly different terminology, the official joint framework[3] describes them as:

1. Command and control, or, as the Army now calls it, mission command. In general terms, command and control (C2) refers to the ability to direct subordinate forces toward a common end;
2. Intelligence, or the ability to gather, synthesize, and distribute information about the operational environment through both technical (e.g., signals intelligence) and non-technical (human intelligence) means;
3. Fires, or the ability to precisely deliver "effects," be they kinetic (physical) or non-kinetic (e.g., electronic warfare or psychological operations such as deception), on a desired target (which could be a structure, organization, person, etc.);
4. Movement and manoeuvre, or the planned and regulated movement of military forces toward an objective;
5. Protection, or the ability to avoid and/or defend against attacks, both kinetic and non-kinetic. This can refer to individuals, units, bases, pieces of equipment, etc.; and
6. Sustainment, or the ability to provide all classes of supply (e.g., food, ammunition, spare parts, etc.) to forces over time.

Networks (wired and wireless, space-based and terrestrial) play a crucial role in each of these functions. There are dozens of programs, both joint and at the individual military service level, that are intended to provide capabilities in one or more of these functional areas. Indeed, of the seven priority areas listed in the Defence Department's Fiscal Year 2015 budget request, cyber was first. Of the remaining six – missile defence; nuclear deterrence; space; precision strike; intelligence, surveillance and reconnaissance; and counter terrorism and special operations – all either directly support or rely heavily on networked capabilities.

As ICT have developed and created the promise of NEC, they have presented both opportunity and challenge. The opportunity lies in greatly enhanced capability not just within platforms, but across them. One of the

[3] US Dept of Defence, Chairman of the Joint Chiefs of Staff, *Joint Publication 3-0: Joint Operations*, 11 August 2011, http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf.

challenges is injecting that potential across a staggeringly large inventory of equipment. The US Army alone has over ten thousand combat vehicles and helicopters. Replacing or upgrading those systems to "build in" net-enabled architectures is a massive expense, and in some cases is not even possible. The US military now finds itself in a position of some irony. On the one hand, budget pressures make moving to net-enabled equipment fleets much more challenging. On the other, they are even more necessary as funding and associated force reductions demand greater productivity out of existing formations.

Each of the four military services is taking the same basic approach to finding the right balance between budgets and capability enhancements. Funding for new programs is being cut back significantly, but any "new starts" will be designed to be net-enabled, and with open architectures to allow for capability upgrades as ICT continue to advance. Existing equipment is being incrementally upgraded, in some cases to provide sufficient support (especially power) to allow for greater networking among disparate systems and in some cases to insert updated capabilities directly. Models that are either inefficient or unable to be networked are being retired as expeditiously as possible. The Air Force and Navy are largely attempting to "pure fleet" their major weapon systems – e.g., to reduce the number of different models of ships or airplanes and achieve equivalent capabilities across them. The Marine Corps and Army, who typically have very large equipment inventories, must in many cases out of necessity have like-model platforms with differing levels of capability, creating interoperability challenges within their own units for larger scale operations. The intent is to minimize such differences to the greatest possible extent, but fiscal realities have forced the Army in particular to move to more explicit strategy of incremental upgrades across multiple programs, with differing increments across the force. Overall, however, the Army's desire to evolve from "stand alone systems to networked systems"[4] is shared by the entire US military, and all of the services are moving in that direction.

[4] US Dept of the Army, *Army Equipment Program in Support of President's Budget 2015*, May 2014, p. 5, http://www.army.mil/e2/c/downloads/348286.pdf.

1.2 The US Armed Forces' requirements related to NEC

Throughout the modern era, the United States has based its defence strategy on quality over quantity. That approach rests on two assumptions: that the US will have a competitive advantage in access to and use of advanced technologies, and (especially since the Vietnam War era) that highly-trained volunteers will more effectively employ those capabilities than would large, conscripted forces. The advances in ICT are very consistent with the US military's emphasis on quality, as networks offer even greater potential to increase the military productivity of any given unit. That said, the US military recognizes that on the one hand stand-alone capabilities lack synergy, but on the other that networked ones present opportunities for adversaries to achieve much greater effects should they be able to penetrate or deny access to those networks.

Evidence of these concerns can be found in the major investments the US military is making in cyber defences, though those fears are not preventing the full adoption of NEC. In many ways, broad-based recognition of the potential ICT offered for the US military began with Global Positioning System (GPS) satellite navigation system and the positioning, navigation and timing (PNT) information it provides. PNT data have revolutionized every warfighting function, from Blue Force Tracker systems that allow commanders to "see" the positions of each vehicle in their unit in real time to the passing of precise coordinates to munitions to the use of unmanned aerial systems to deliver supplies directly to remote stations in the mountains of Afghanistan.[5] As alluded to above, the revolutionary impact of PNT data on US military operations comes with some risk, however, and not only from cyber attacks. Increasingly, US military leaders have cautioned that space is becoming more and more congested, and also more contested. This poses a significant threat (purposeful or otherwise) to every aspect of US military operations, from communications to intelligence to the provision of logistic support. Most notably, it raises the prospect that GPS links could become unavailable. There are multiple efforts underway to mitigate these risks, but with respect to GPS reliance in particular, the US

[5] See Lockheed Martin, U*.S. Marine Corps to Keep K-Max Unmanned Cargo Re-Supply Helicopter in Theater for Second Deployment Extension*, 31 July 2012, http://lmt.co/1F88Va1.

is examining a range of options. These include programs aimed at applying microtechnologies to enhance access to PNT data, as well at developing alternatives approaches to GPS-supplied navigational fixes.[6]

While PNT information has been revolutionary in many ways, US military requirements for NEC now extend much further. The current Chief of Naval Operations, Admiral Jon Greenert, has long been vocal in his view that the network is no longer a supporting function, but has become so central that it is a combat system in its own right.[7] The Navy's perspective on this is reflected in major organizational changes combining responsibilities for intelligence and communications capabilities and oversight. The Air Force, the most technologically-inclined service, has been less explicit in articulating the centrality of NEC to its operations, but its responsibilities for space capabilities, its early sensitivity to myriad cyber issues, and its steps to enhance aerial layer communications networks illustrate that it is of like mind with the Navy. For the Army, the past decade-plus of combat operations have convinced all of its senior leaders that the ability to see themselves and the enemy, and to rapidly push that information around the battlefield, are crucial, and that all of this rests on robust networks. Army leaders routinely state, in words that are reflected in the service's budget, that the network is the number one acquisition priority. The Marine Corps, which draws most heavily on support from the other services, also recognizes that NEC offer vastly increased capability within its own formations, and are central to its interactions with the rest of the joint force. Thus while ICT specifics continue to rapidly evolve, there is consensus across the US military that its future success rests on the continued ability to better leverage those advances with NEC.

[6] See, for example, in the website of the Defence Advanced Research Projects Agency (DARPA): Robert Lutwak, *Micro-Technology for Positioning, Navigation and Timing (Micro-PNT)*, http://www.darpa.mil/program/micro-technology-for-positioning-navigation-and-timing; Lin Haas, *Adaptable Navigation Systems (ANS)*, http://www.darpa.mil/program/adaptable-navigation-systems. In addition to these two Defence Department research efforts, the Army is pursuing a four-part program designed to enhance the protection of GPS signals and diversify the sensors from which signals could be provided. See Justin Doubleday, "Congress approves Army funding for 'assured' navigation technology", in *InsideDefense.com*, 10 October 2014.

[7] Henry Kenyon, "Navy views network infrastructure as a vital combat component", in *DefenseSystems.com*, 9 June 2011, http://defensesystems.com/articles/2011/06/09/naval-it-day-greenert-network-as-combat-system.aspx.

At the same time, there is also recognition that others have many of the same opportunities. US advances in precision fires have not been unique, and the US military is increasingly focused on emphasizing dispersed or distributed operations in which units are disaggregated as needed and then able to rapidly re-aggregate to employ the benefits of mass at the right time and location. This emphasis is particularly strong in US ground forces: increasing training for distributed operations is the Commandant of the Marine Corps' third priority,[8] and "operating decentralized" was one of seven supporting ideas in the previous Army Operating Concept.[9] In fact, both services have recently issued updated documents outlining their visions for how they will operate in the future, and NEC can be found throughout.

In March 2014, the Marine Corps released its latest capstone concept entitled Expeditionary Force 21 (sometimes referred to as EF 21).[10] EF 21 provides the Corps' vision of the future, and serves as the overarching vision to inform future force development. It restates the Marine Corps' intent to focus on crisis response as its primary mission, and to restoring its expeditionary heritage.[11] The document describes an approach that emphasizes greater forward presence, increased regionally-specific expertise, greater ability to "scale" command and control and assigned

[8] US Marine Corps, *Service Campaign Plan for 2014-2022*, 21 May 2014, https://marinecorpsconceptsandprograms.com/sites/default/files/files/United%20States%20Marine%20Corps%20Service%20Campaign%20Plan%202014-2022.pdf.

[9] US Army Training and Doctrine Command (TRADOC), *The United States Army Operating Concept, 2016-2028*, TRADOC Pamphlet No. 525-3-1, 19 August 2010, p. 17, https://fas.org/irp/doddir/army/opcon.pdf. It is less explicitly called out in the most current version, but it is still a key element of the Army's plans. US Army Training and Doctrine Command (TRADOC), *The U.S. Army Operating Concept: Win in a Complex World, 2020-2040*, 31 October 2014, TRADOC Pamphlet No. 525-3-1, 31 October 2014, http://www.tradoc.army.mil/tpubs/pams/tp525-3-1.pdf.

[10] US Marine Corps, *Expeditionary Force 21. Forward and Ready: Now and in the Future*, 4 March 2014, http://www.mccdc.marines.mil/Portals/172/Docs/MCCDC/EF21/EF21_USMC_Capstone_Concept.pdf.

[11] This reflects the Marine Corps' concern that operations in Iraq in particular and Afghanistan to some degree have required the Corps to be more stationary and tied to fixed infrastructure than its institutional heritage, culture, and assigned missions might suggest are desirable. One reflection of this concern is the frequent claim that a "generation of Marines" did not deploy on ships, and that the knowledge and skill sets associated with operating from the sea must be rebuilt.

forces from very small to relatively large operations, rapid deployment of task-organized and distributed forces, enhanced capabilities to operate in complex electro-magnetic environments (with associated technologies), and greater integration with special operations forces.

The Marine Corps' concept was followed in October 2014 by the Army's updated Army Operating Concept, or AOC.[12] The AOC is also intended to guide future force development, and places a new emphasis on setting the theatre as well as actions taken to shape the security environment. It also stresses how integral joint and combined operations will be to future Army operations, arguing that "Army forces are uniquely suited to shape security environments through forward presence and sustained engagements with allied and partner land forces."[13] The concept also specifically calls out communications and information processing technologies as helpful in developing common operational pictures and reducing technological complexity for users.[14] While it does not explicitly acknowledge the centrality of NEC to its success, the AOC's central idea envisions "globally responsive combined arms teams maneuver[ing] from multiple locations, […] tailored rapidly to the mission, […] and integrat[ing] joint, interorganizational, and multinational capabilities."[15]

For both the Marine Corps and the Army, realizing their visions for how they will conduct future operations will necessitate even greater reliance on ITC specifically and NEC more broadly. A more detailed discussion of implications by warfighting function helps to further illustrate this fact.

Command and control. The ability of ground combat leaders to communicate and direct their forces is the foundation of effective operations, and, in the eyes of both the Army and Marine Corps, is inherently reliant on networks.[16] As the Army's senior general for future force development

[12] US Army Training and Doctrine Command (TRADOC), *The U.S. Army Operating Concept: Win in a Complex World*, cit.

[13] Ibid., p. 8.

[14] Ibid., p. 13.

[15] Ibid., p. 15.

[16] The Marine Corps' C2 vision, for example, says that C2 is "leader-centric, *network-enabled* (emphasis added), and is intended to support the continuous decision-making cycle of commanders at every level to ensure they are positioned to best plan, direct, coordinate and control." US Marine Corps, *USMC Concepts and Programs 2013*, http://www.hqmc.marines.mil/pandr/ConceptsandPrograms/ConceptsandPrograms2013.aspx. The Army Mission Command Strategy says that "The network and various other technological sys-

has stated, the Army's top investment priority is the continued development of wireless networks. The Army sees those networks, which enable communications down to the platoon, squad, or even individual level, as foundational to the construction and updating of shared situational understanding from which all command and control activities flow.[17] For ground forces in particular, command and control concepts now take for granted that commanders at every echelon will have basic (but precise) information about the units above, adjacent to, and subordinate to them. They also assume that commanders will have multiple, redundant communications channels to enable increasingly decentralized operations. In addition, various Defence Department entities are examining how best to leverage developments in ever-smaller, networked sensors, looking to automate the collection and visualization of additional data about units, to include down to the individual level. For example, the Defence Advanced Research Projects Agency is pursuing an integrated approach to networking various soldier-based technologies that would automatically provide data about service members' health status (e.g., temperature, oxygen levels, or hydration) or logistics status (e.g., amounts of ammunition expended).[18] The Marine Corps also identifies ICT as a key C2 enabler, noting that

> [g]iven the anticipated complexity, tempo, and distributed nature of future power projection operations, naval forces will require both advanced information technology and flexible command relationships to support an increased level of coordination and integration among all elements of the force.[19]

tems are key parts of a commander's [mission control] system." US Army Combined Arms Center, *U.S. Army Mission Command Strategy, FY13-16*, June 2013, http://usacac.army.mil/cac2/Repository/Army_Mission_Command_Strategy_dtd_12June%202013.pdf.

[17] Sydney J. Freedberg, "The Army gropes toward a cultural revolution", in *Breaking Defense*, 22 October 2014, http://breakingdefense.com/?p=16597.

[18] See Scott Maucione, "DARPA wants white papers on 'Squad X' dismounted info-sharing", in *InsideDefense.com*, 31 July 2014.

[19] US Marine Corps, *Expeditionary Force 21*, cit., p. 33. EF 21 goes on to identify a number of necessary supporting capabilities, to include specific requirements associated with enhanced robustness of communications, the ability to support collaborative planning and decision making, improved interoperability and security, and better access to timely information from outside sources.

Operations in Iraq and Afghanistan, which involved many small units operating in very remote locations and over large areas, highlighted the need for US ground forces to enhance their ability to be "connected" at the lowest possible levels. To that end, both the Army and Marine Corps have been pursuing technologies to enable network connections not only for larger deployed headquarters but also "to the edge." Both recognize that commercial ICT development will continue to drive rapid advances in capabilities, but their plans to harness that reality differ.

With respect to future communications, in broad terms the Army's approach to providing operational and tactical connectivity is based on common waveforms. The basic concept is that the US Defence Department would specify standards for waveforms, as well as for the protocols for network management and information encoding. These standards would then allow companies to design both hard- and software around those waveforms, which could also be portable from device to device.

The Marine Corps, on the other hand, has determined that trying to drive suppliers toward specific waveforms is uneconomical and unrealistic. Instead, they are pursuing advances in processing power and reprogrammable software to support rapid translation of varied waveforms across different pieces of equipment.[20] To that end, they have been experimenting with creating network "bridges" among vehicles to aerial platforms, pushing digital interoperability that leverages existing equipment.

There are some indications that the Army, which has faced some technical and fiscal challenges in programs designed around specified waveforms, is now considering a more commercially based approach. For example, in September 2014, the Army's electronics research centre indicated plans to evaluate whether fourth-generation Long Term Evolution (4G LTE) technology can meet its battlefield communications and intelligence needs.[21]

Both services are also pursuing ways to increase paths of information sharing and connectivity. For example, in 2013 the Marine Corps demon-

[20] Matthew Glavy, "The Flight MAP: The Marine Aviation Plan Through 2040", in *CSIS Events*, 28 April 2014, http://csis.org/node/48793.

[21] Bob Brewin, "Army Eyes 4G Cellular Tech for Combat Communications", in *Nextgov*, 10 September 2014, http://www.nextgov.com/defense/2014/09/army-eyes-4g-cellular-tech-combat-communications/93689.

strated and intends to further develop the capability for forces to get real-time intelligence updates while en route to long-distance missions aboard V-22 tilt-rotor aircraft,[22] combining communications and intelligence to better inform operators. The Marines are pursuing additional applications to take greater tactical advantage of planned big data cloud environments,[23] and the Army is focused on investments aimed at enhancing the convergence between its operations and intelligence networks.[24]

In addition to ground-based operations, the Marine Corps is also placing a greater priority on enhancing its C2 relationships (and supporting capabilities) with other naval elements, both US Navy and Coast Guard. To better support scalable forces, they are emphasizing enhancing existing relationships at the operational level with greater experimentation and exercises at lower echelons, as well as on higher-level planning staffs.[25]

Intelligence. ICT advances are absolutely essential to future intelligence needs. The wars in Iraq and Afghanistan drove substantial progress in the integration of "all-source" intelligence data from human, signals, geospatial, and other sources. This lead to a range of new tools designed to make intelligence faster and more relevant to military commanders at all levels. From the onset of the conflicts, US Special Operations Forces developed and refined processes, through network-based analysis enabled by networked systems, to rapidly find targets of interest, fix them in a given position, and "finish" them with raids or seizures. These raids also produced additional forensic data (both physical and virtual) that was fed back into the intelligence cycle, leading to additional target "finds," and so on. These processes were expanded to conventional forces as well, and are becoming increasingly routine across US ground units.

The ability to pass intelligence information at multiple levels of classi-

[22] Amy Butler, "USMC to outfit Ospreys with comms node", in *Aviation Week & Space Technology*, 14 October 2013, http://aviationweek.com/node/4026.

[23] Bob Brewin, "The Navy wants a tactical cloud", in *Defense One*, 25 September 2014, http://www.defenseone.com/technology/2014/09/navy-wants-tactical-cloud/95129.

[24] US Senate, Committee on Armed Services, Subcommittee on AirLand, *Statement of Gen. John F. Campbell, Vice Chief of Staff, United States Army, on Fiscal Year 2015 Ground Force modernization and individual equipment modernization programs*, 9 April 2014, http://www.armed-services.senate.gov/imo/media/doc/Campbell-Barclay-Williamson_04-09-14.pdf.

[25] See US Marine Corps, *Expeditionary Force 21*, cit., p. 29-30.

fication, as well as to integrate and visualize it in new ways, has been truly transformational for US ground forces. Greater understanding of their own forces, coupled with much greater insight into local populations and adversaries, have given commanders better situational awareness than previous generations could likely have imagined. Challenges remain with hosting data with different levels of classification, and with data sharing across coalition partners, but many of these issues are based on policy rather than technology.

Fires. NEC have also unlocked joint fires in previously unimaginable ways. The addition of kits incorporating laser or GPS guidance to air-, sea- and ground-based systems, coupled with the build-out of communications networks, has meant ground commanders can now "call for fires" from numerous platforms, with extremely high confidence in their accuracy. Networked intelligence systems allow for much more diverse and well-developed targets, and sensor-to-shooter fusion allows ground forces to simultaneously conduct intelligence and strike operations and to pair manned- and unmanned-systems in new ways. The Army, for example, is fielding systems that allow attack helicopter pilots to control unmanned air vehicles from their cockpits, as well as to monitor video feeds from the drones as well as from Air Force platforms directly.[26] Further, some in the fires community are positing that new, narrow-band satellite communications capabilities could offer robust command and control links, enabling tactical-level fires from various artillery or rocket systems.[27]

Perhaps the most significant implication of ICT in the fires arena is the degree to which they create the potential for both kinetic and non-kinetic fires. Though barriers (many of them cultural) to the full integration of non-kinetic fires such as electronic warfare, cyber, and information operations remain, they are (arguably) slowly breaking down. The Army electronic warfare community, for example, is being reconstituted and is dedicated to developing a broader suite of capabilities than those developed specifically to counter the threat of improvised explosive devices

[26] Paul McCleary, "US Army Presses Ahead on Manned-Unmanned Teaming", in *Defense News*, 30 April 2013, http://www.defensenews.com/article/20130430/DEFREG02/304300018.

[27] Patrick A. Schrafft, "Enhancing fires with next-generation narrowband SATCOM", in *Fires*, July-August 2014, http://www.readperiodicals.com/201407/3410820761.html.

(IEDs) in Iraq and Afghanistan. Both services have developed new organizations (the Cyber and Electronic Warfare Coordination Cell, or CEWCC, for the Marine Corps and the Cyber Electromagnetic Activities, or CEMA, cell for the Army) to help better integrate non-kinetic fires both internally and within ground units' fires activities. Harnessing the potential requires netting some existing capabilities together (e.g., individual Army jammers), but also continuing to evolve the organizations and doctrine so that commanders fully appreciate and utilize non-kinetic tools in support of their overall scheme of manoeuvre.

Movement and manoeuvre. As discussed above, NEC have had a dual effect on movement and manoeuvre. The advances in precision they enable are not restricted to US forces, which have forced the Army in particular to update its previous conceptions of mass. They also have enabled the Army and Marine Corps to consider new ways in which they might allow ground forces to disaggregate and regroup for operational advantage. Beyond the ability of units to coordinate their movements more effectively, ICT and NEC have had major effects on the evolution of the combat vehicles that support manoeuvre. Each major wheeled and tracked platform (i.e., tank) has undergone multiple upgrades to enhance its ability to generate and pass data, continuously bumping up against size and power constraints. Yet the degree to which US ground forces view networked capabilities as essential to their operations is evident in the requirements they set forth for all future ground vehicles, both wheeled and tracked. Each has space dedicated to NEC, and requirements to maximize the ability to conduct upgrades through software refreshes, many of which are intended to further tie vehicle systems to networked information. US ground forces also continue to pursue NEC that better synthesize existing data sources, from integrated display and targeting systems for tank commanders to data links enabling programmable tank rounds to deployable terminals to view drones' video feeds.[28]

Movement and manoeuvre is not restricted to high-end combat operations. It also applies to the training and exercises and other activities that the Army now characterizes as "shaping the security environment." NEC are equally relevant to movement and manoeuvre in this context. For ex-

[28] US Marine Corps Systems Command, *Modern Day Marine: Report to Industry*, 25 September 2014.

ample, the Marine Corps recently decided to field an Android-based app for its civil affairs units. The app allows them to electronically capture, process and share information about the condition of local infrastructure such as water and sewer systems, schools, or roads during humanitarian assistance operations, facilitating the more efficient and effective delivery of aid.[29]

Protection. Ensuring US ground forces have sufficient protection is intrinsically tied to the other warfighting functions, as doctrine says US ground forces will use (network-enabled) intelligence and command and control to manoeuvre in ways that avoid potential threats, using information advantages such as precision fires to neutralize them. Dispersal's increasing centrality to US conceptions of protection is also predicated on assured communications and connectivity. Both rely on NEC such as active and passive sensor networks to provide threat information, and use ICT to process that data into visual displays for both mounted and dismounted personnel. As just one example, at the individual service member level, the Army and Marine Corps are both exploring sensors in helmets that could provide information on the locations and severity of head injuries, a recognition of the occurrence of traumatic brain injury over the past decade-plus.

In addition to protecting themselves, ground forces play an integral role in protecting other forces and civilian populations. The Army's Patriot missile defence system has been among the most requested assets in recent years, and the Army is pursuing kits that would allow those systems to plug into a networked missile defence architecture incorporating multiple weapons and sensors.[30] And both the Marine Corps and Air Force versions of the F-35 Joint Strike Fighter, which rely on precision targeting and munitions as well as networked data about friendly force locations, are intended to provide enhanced close air support to all ground forces in the future.

Sustainment. Long lines of communication in Afghanistan and Iraq have generated a new focus on decreasing US sustainment requirements

[29] Barb Hamby, "Fielding decision made on new civil affairs app", *Marine Corps Systems Command Press Release*, 9 October 2014.

[30] Justin Doubleday, "Army seeks info on Patriot-interface kits for networked missile defense", in *Inside the Army*, 3 October 2014.

(e.g., reducing reliance on fuels and batteries) but also on alternative ways to conduct logistics support. Prior to the wars, there was a greater focus on pursuing NEC that enabled increased efficiency and transparency in the logistics process through technologies such as RFID chips. While both the Army and Marine Corps remain committed to improving supply chain operations, the wars have generated a much more robust exploration of robotics and other unmanned systems' abilities to help with sustainment, all utilizing NEC. For example, in 2011 the US Marine Corps deployed the unmanned K-MAX helicopter to Afghanistan for supply operations. It was sufficiently successful that operators in theatre expanded upon its capabilities, and both the Marine Corps and Army are evaluating whether it should become a formal service program.[31] To further complement the benefits of the platform, the Marine Corps has also been participating in developing an automated control system based on advanced algorithms and sensor networks that allow the K-MAX or other aerial platforms to be operated autonomously and in austere environments.[32] The Army and Air Force have also both contributed technologies to develop the Joint Precision Air Drop System (JPADS), a GPS-guided parafoil capable of precise delivery of varying payloads.[33]

Key enablers. As noted above, there is broad recognition that almost every aspect of US military operations relies on the integrity of networks and the information that travels along them, and increasingly so every day. Maintaining that integrity has multiple dimensions, as it requires adequate defences against disruptions as varied as cyber attacks, crowded electromagnetic spectrum, and increasing amounts of space debris. Within the US military, there are shared responsibilities to ensure those defences among functional combatant commanders (especially US Strategic and Cyber Commands) and each of the military services, to varying degrees.

Twin phenomena have contributed to heightened anxiety about po-

[31] Mike Hoffman, "Marines Work to Extend K-MAX in Afghanistan Through 2014", in *DefenseTech*, 25 September 2013, http://defensetech.org/2013/09/25/marines-work-to-extend-k-max-through-2014.

[32] Kris Osborn, "Marines fly helicopters with mini-tablet", in *DoD Buzz*, 5 April 2014, http://wp.me/pgSCu-8kt.

[33] "JPADS: Making precision air-drops a reality", in *Defense Industry Daily*, 27 April 2014, http://www.defenseindustrydaily.com/?p=678.

tential U.S vulnerability to network interruptions. The first is the growing dependence on NEC, a consistent theme in this paper. All of the military domains recognized in US joint doctrine – air, land, sea, space, and cyber – not only rely on but also play key roles in facilitating NEC. Speaking about one of those domains, one Defence Department official recently noted that

> In the past 25 years, space capabilities have become […] a commodity service whose presence we take for granted until the moment its availability is interrupted. Our dependence on space has become inextricably linked to our other critical capabilities.[34]

This holds true for the EMS more broadly (which supports wireless connectivity and electronic warfare) and of wired networks as well. Indeed, the Army Science Board recently noted that the Army will be challenged to mitigate "digital vulnerabilities […] owing to U.S. reliance on digital systems," and that it needs to develop a "counter-digitization" concept to both address that reality and to exploit that same reliance in adversaries.[35]

The second contributing factor to growing discomfort over network reliance has been a concern that the conflicts in Iraq and Afghanistan may have bred some form of complacency or overconfidence. In both conflicts, US forces enjoyed near-total dominance of the air and space domains in particular. Activities in the maritime domain were limited. The cyber domain was somewhat more contested, especially by remotely controlled Improvised Explosive Devices, or IEDs. The most challenging elements of both conflicts, however, have taken place in the land domain. The wars highlighted key interoperability challenges among the US services as well as multinational partners, and in some cases offered the opportunity to resolve them.[36] However, the lack of a highly capable adversary meant that coalition forces could emerge from these conflicts with a higher de-

[34] US House of Representatives, Armed Service Committee, Subcommittee on Strategic Forces, *Statement of Gil I. Klinger*, 3 April 2014, p. 9, http://docs.house.gov/meetings/AS/AS29/20140403/102037/HHRG-113-AS29-Wstate-KlingerG-20140403.pdf.

[35] Army Science Board, *Decisive Army Strategic and Expeditionary Maneuver*, 18 September 2014.

[36] Sydney J. Freedberg, "What the US, NATO must do to counter Russia: Breedlove, Gorenc & Odierno", in *Breaking Defense*, 22 September 2014, http://breakingdefense.com/?p=15930.

gree of confidence about the resilience of their NEC than would be the case against a more advanced competitor.

To attempt to correct for what many see as a false, and dangerous, sense of complacency, the US military is renewing its focus on training and preparing for less benign environments, especially in the air, maritime, and cyber domains. This concern explains, at least partially, the emergence of a strong focus on "anti-access, area denial" (A2/AD) threats. These include long-range missiles, but also highly skilled cyber opponents, possible anti-space challenges, electro-magnetic pulses, and other advanced capabilities that would negate key US technological advantages.

From a space perspective, US officials evidence increasing concern both about space clutter and adversary counter-space capabilities, which are driving a strategy based on increasing US resilience in space. This strategy has three main elements. The first is to increase space situational awareness by pursuing information sharing agreements with commercial companies and other governments who have PNT capabilities to help ensure US access in the event of a compromise.[37] Such agreements also require modifying equipment so that it can receive signals from others' space navigation systems.[38] The second element of the strategy is to seek greater dispersion of US space assets (to include smaller payloads on multiple commercial and military vehicles). The final element is to enhance the reliability of existing platforms such as GPS, the suite of Wideband Global SATCOM (WGS) satellites, the Space-Based Infrared System (SBIRS), which is a six-satellite constellation supporting early warning and missile defence, and the Advanced Extremely High Frequency, or AEHF, four-satellite constellation that provides robust communications capabilities. The US also continues to pursue defences against electro-

[37] By spring 2014, the US had signed agreements with Australia, Japan, Italy, Canada and France, and had agreements with 41 commercial satellite operators. US House of Representatives, Armed Service Committee, Subcommittee on Strategic Forces, *Statement of Douglas L. Loverro*, 3 April 2014, http://docs.house.gov/meetings/AS/AS29/20140403/102037/HHRG-113-AS29-Wstate-LoverroD-20140403.pdf. In August, US Strategic Command signed another data sharing agreement with the European Organization for the Exploitation of Meteorological Satellites. Jordana Mishory, "Stratcom signs new space situational awareness data-sharing agreement", in *Inside the Pentagon*, 4 September 2014.

[38] US House of Representatives, House Armed Service Committee, Subcommittee on Strategic Forces, *Statement of Douglas L. Loverro*, cit., p. 8.

magnetic pulses (EMPs), after a long series of Congressionally-directed commissions and internal Defence Department analyses that have consistently highlighted the potential damage an EMP could cause.[39]

In addition to pursuing a more diverse and robust satellite communications capability, the US military is interested in enhancing the overall communications architecture to allow for continued connectivity if any given layer (e.g., satellite) becomes unavailable. One of the stated benefits of an unmanned aerial communications layer, for example, is that it provides backup capacity if satellite communications fail.[40] This rationale is partially driving the Marine Corps' strong push to enhance digital interoperability amongst its platforms.

As noted earlier, there are also major investments being made in improving the US military's cyber security. US Cyber Command has established a Cyber Mission Force (CMF) with three component forces, a National Mission Force to protect US national networks, a Cyber Combat Mission Force to support the cyber needs of regional combatant commanders, and the Cyber Protection Force to defend Defence Department networks.[41] The Army, Navy and Air Force are collectively contributing trained cyber operators to build a total of 133 CMF teams. For ground forces in particular, the Army and Marine Corps are also developing cyber operators to support units below the combatant command level.

On the acquisition side, the US Defence Department has developed the Joint Information Environment, or JIE, which is a standard, open network architecture based on a common infrastructure and supporting processes and policies. One of the JIE's core objectives is to support increased interoperability among the US military services, as well as to enhance cybersecurity.[42] In addition to developing regional security stacks, JIE is also facilitating the development of "unified capabilities," an effort between the Defence Information Systems Agency, the Army, and the Air Force to

[39] James Jay Carafano and Richard Weitz, "EMP attacks: What the U.S. must do now", in *Heritage Foundation Backgrounder*, No. 2491 (17 November 2010), http://www.heritage.org/research/reports/2010/11/emp-attacks-what-the-us-must-do-now.

[40] Army Science Board, *Decisive Army Strategic and Expeditionary Maneuver*, cit.

[41] Cheryl Pellerin, "Cybercom activates national mission force headquarters", in *DoD News*, 25 September 2013, http://www.defense.gov/news/newsarticle.aspx?id=120854.

[42] Jordana Mishory, "DoD eyes interoperability in next-gen host-based cybersecurity strategy", in *Inside the Pentagon*, 21 August 2014.

pursue voice, video and data tools that could be used across the US military enterprise. The Army is leading the unified capabilities effort, which is expected to include the expansion of chat services like those heavily utilized in Iraq and Afghanistan to a broader set of users.[43]

At the service level, EF 21 emphasizes that "[f]reedom of action in cyberspace and the electromagnetic spectrum (EMS) is a key enabler to 21st century military operations."[44] Though not expressed as succinctly, that same view is shared by the Army, which over the past year has established a new Cyber Centre of Excellence, integrated electronic warfare within that Centre, and created a new military branch for cyber personnel, the first new branch since the creation of special forces in the late 1980s. While both services continue to evolve their organizational structures that govern responsibilities for cyber and spectrum, clear steps are being taken to increase their prominence (both defensive and offensive) in future operations.

1.3 Relevant procurement programs related to NEC

Every major program has embedded NEC. Some programs are explicitly designed to provide networks, while others indirectly leverage NEC to enhance their overall performance. While by no means comprehensive, the following section reviews some of the major ground force programs that relate most directly to NEC, again by warfighting function.

Command and control (C2). Both the Army and Marine Corps participate, to varying degrees, in multiple joint programs related to leveraging NEC for C2. One is the Joint Battle Command-Platform (JBC-P), the principal command and control and situational awareness tool for Army and Marine Corps forces at the brigade level and below. It is a developmental program intended to form the foundation for future joint force situational awareness, and is being developed by the Army's Software Engineering Directorate in Huntsville, AL. Another multi-billion dollar effort is the

[43] Justin Doubleday, "Solicitation eyed this fall for 'unified capabilities' networking tools", in *Inside the Army*, 19 September 2014.

[44] US Marine Corps, *Expeditionary Force 21*, cit., p. 35-36.

Joint Tactical Radio System, or JTRS, now known as the Family of Networked Tactical Radios. Originally an ambitious vision of fully interoperable radios with exportable waveforms, the program has faced both cost and schedule challenges, and was restructured in 2011. The current Family of Networked Tactical Radios effort is intended to produce multiband, multi-mode radios using IP-based technologies from numerous participating vendors. One component of the restructure is the Handheld, ManPack, and Small-Form Fit program, for which contracts being sought by General Dynamics, Rockwell Collins, Thales, and Harris Corporation. One key element is the ManPack radio, a backpack portable version that has faced multiple challenges. In June 2014, the Army suspended fielding of General Dynamics' proposed radio because of concerns about weight, overheating, range, and power consumption. General Dynamics has responded by self-funding the development of an improved version, though it remains unclear whether this option will win out over competing designs.[45] The Army expects to issue a formal request for proposals for the ManPack version at some point in the first half of 2015. It did so in early 2015 for the handheld radio version, known as Rifleman, and plans to issue multiple contract awards to various competitors for the test phase before further downselects for production. In the meantime, to address JTRS delays the Marine Corps began a program called Tactical Communications Networking (TCN), a family of radios to support voice and data communications for deployed forces. Finally, the two services are collaborating on the Joint Battle Command-Platform (JBC-P) program, the primary C2 and situational awareness software application at the brigade level and below. Multiple companies, to include DRS Technologies and General Dynamics, are involved in the effort.

Beyond joint programs, the Army and the Marine Corps have additional service-specific programs aimed at further enhancing their NEC. One major component of the Army's network strategy is the Warfighter Information Network-Tactical (WIN-T) program, a General Dynamics-built system that provides voice, data and video communications either terrestrially or through satellite links.[46] The current increment provides

[45] Sebastian Sprenger, "General Dynamics launches "Apollo" in bid to save its Army radio business", in *Inside the Army*, 3 October 2014.

[46] "Bringing situational awareness to the battlefield", in *C4ISR & Networks*, 18 August

an initial on-the-move capability, as well as larger data pipes at higher echelons. Subsequent increments are intended to increase transmission robustness, ultimately through an aerial layer. That said, the Defence Department testing organization continues to have concerns about the program's instability, complexity, reliability and range.[47] The Army shares some of those concerns, and senior officials have discussed the potential of stretching out or restructuring the program if issues persist.[48] Budgetary pressures are also contributing to slowing WIN-T fielding.

Another key program is Nett Warrior, a dismounted soldier mission command system that provides command, control and situational awareness to individual squad members. A small commercially based device that connects to the network through radios, Nett Warrior is the program through which the Army will seek to converge handheld devices into a single technology. Army engineers serve as the prime integrator; multiple companies, including Samsung, ADS Inc., and General Dynamics, provide components.

For the Marine Corps, in addition to the TCN, another primary initiative is the development of the Common Aviation Command and Control System (CAC2S). CAC2S is a combination of hardware, software, and facilities intended to support the integration of information from existing air platforms (Marine Corps as well as other services, both manned and unmanned) to facilitate their collective command, control, and coordination. The prime contractors are General Dynamics and Raytheon.

Network-enabled C2 programs are also areas of significant interest for the Navy and Air Force. One of the Navy's largest efforts in this area is the Consolidated Afloat Networks and Enterprise Services (CANES) program. CANES is the next generation tactical afloat network for Navy ships (to include the amphibious ships employed by the Marines) and submarines, and is being supported by BAE, General Dynamics, Global Technical Systems, Northrop Grumman, and Serco. The Navy is also looking for more robust space access from its Navy Multiband Terminal program, built by

2014, http://www.c4isrnet.com/article/20140818/C4ISRNET06/308180005.

[47] US Dept of Defence, Director Operational Test and Evaluation, *Reasons behind program delays: 2014 update*, 26 August 2014, http://www.dote.osd.mil/pub/presentations/ProgramDelaysBriefing2014_8Aug_Final-77u.pdf.

[48] Sebastian Sprenger, "Army may break up major network program if results fall short", in *InsideDefense.com*, 14 October 2014.

Raytheon. The Air Force's airborne C2 efforts include pursuit of a next generation JSTARS (Joint Surveillance and Target Attack Radar System), utilizing a commercially available airframe. Northrop Grumman builds the current platform, but numerous competitors are expected for the future program. The Air Force intends to ensure that platform is capable of easily integrating new sensors, computers, avionics, and other electronic systems as they are developed.

Intelligence. Across all of the services, the major intelligence programs are all aimed at increasing the ability for forces to leverage multiple intelligence data sources. All are involved in the development and fielding of the Defence Common Ground System (DCGS); the Army and Marine Corps versions are referred to as DCGS-A and DCGS-MC, respectively. DCGS is a large-scale program with multiple functionalities, to include intelligence processing, exploitation, analysis, and production. The Army's version in particular has come under strong criticism for being inflexible and difficult to use, though Army leadership continues to back the program and encourage integration of new capabilities.[49] Multiple companies are participating, including Lockheed Martin, General Dynamics and Northrop Grumman, and the overall program is projected to cost tens of billions when complete.

All of the services also participate in the Tactical Exploitation of National Capabilities, or TENCAP, program. TENCAP focuses on developing tools that enable small units to draw upon satellite and other national-level intelligence capabilities. TENCAP includes numerous programs and systems, with participation by most of the major US defence contractors.

The Army continues to develop Boeing's EMARSS (Enhanced Medium Altitude Reconnaissance and Surveillance System) program, a manned aerial intelligence, surveillance and reconnaissance capability. Planned improvements include adding a real-time, networked multi-sensor collection suite, focused on operations at brigade level and below.

Fires. Every service's programs to support the delivery of kinetic, and increasingly non-kinetic, fires are based on harnessing network advantages. The Army, for example, is leveraging the WIN-T program mentioned above to support greater dispersion among its artillery, most recently by

[49] For example, the Army is actively seeking vendor input on how best to improve DCGS-A's software and visualization capabilities for Increment 2, the contract for which will be awarded in 2016. "Feedback Sought", in *Inside the Pentagon*, 21 August 2014.

utilizing satellite communications to pass digital data across ranges that allowed for an up to ten-fold increase in the speed of fires delivery.[50] And both the Army and Marine Corps are partnered in the NEC-based Advanced Field Artillery Tactical Data System (AFATDS) family of systems, a Raytheon-produced automated fire support command and control system utilizing digital data communications links. The system supports the integration of artillery, rockets, mortars, naval surface fire support, and close air support at multiple echelons.

The Air Force and Navy are similarly interested in harvesting NEC advances for their respective fires roles. Though details are sparse because of classification, the Air Force's Long-Range Strike Bomber (LRS-B) is the intended replacement for the current bomber fleet. The contract will likely be awarded to either the team of Boeing and Lockheed Martin or to Northrop Grumman. This program also includes a "family of systems," though its precise form is not clear. Some analysts suggest that it may be an integrated system of manned and unmanned aircraft and missiles,[51] which would entail significant NEC demands. Alternatively, the family could include "optionally manned" platforms that could be flown with or without a pilot, or a series of platforms of different sizes. The Air Force plans for the program to reach Initial Operating Capability by the mid-2020s. This suggests that the program will seek to leverage the most advanced ICT available in the short term, but also that it will rely on architectures that allow for major ICT advances to be inserted over time. For its part, the Navy has been heavily focused on two major technological advances in the fires arena: lasers and electro-magnetic rail guns. Both seek to leverage networked information in target acquisition and firing.

Movement and manoeuvre. While their ambitions for pursuing new programs have been dampened by resource pressures, both the Army and Marine Corps continue to develop new platforms for both ground and air. None are explicitly motivated by NEC potential, but all are intended to leverage ICT advances. The Army is pursuing a number of vehicle

[50] Kevin McCaney, "Mobile satellite network gives Army swift artillery support", in *DefenseSystems.com*, 2 December 2014, http://defensesystems.com/articles/2014/12/02/army-win-t-satellite-artillary-support.aspx.

[51] Stew Magnuson, "Top secret Air Force bomber program moves forward", in *National Defense*, September 2014, http://www.nationaldefensemagazine.org/archive/2014/September/Pages/TopSecretAirForceBomberProgramMovesForward.aspx.

programs, to include the Armoured Multi-Purpose Vehicle (AMPV) (BAE Systems), the Paladin Integrated Management (PIM) program (BAE Systems), and the Joint Light Tactical Vehicle (JLTV) (AM General, OshKosh Defence, and Lockheed Martin) all of which are deemed "significant priorities."[52] The Army also wants to develop a new Infantry Fighting Vehicle to replace its aging fleet of Bradley tanks, but has had to delay it due to funding shortfalls.

The Marine Corps is participating in the JLTV program (to replace Humvees) but also needs to replace aging fleets of amphibious assault vehicles. The Corps had originally intended to pursue one vehicle optimized for ship to shore transport (with some ability to fight on land) and another that would have much more ground mobility but more limited swim capabilities. For affordability reasons, the Corps has now decided to delay a new vehicle that would travel at high water speeds over longer ranges and instead focus on the Amphibious Combat Vehicle, or ACV. Further, it has adopted an incremental strategy to purchase multiple ACV variants, the first of which will draw heavily from mature technologies. The vendors are not yet determined, though the Corps has explored both US and foreign alternatives.

On the air side, in 2014 the Army unveiled a plan to reduce the number of helicopter models from seven to four, change their distribution between active and reserve component units, and revamp helicopter pilot training. The plan keeps the most modern airframes in the fleet and divests some of the oldest, least NEC-capable. It also continues upgrades of the AH-64 Apache attack helicopter fleet, built by Boeing, to the "E" model. The upgrade involves the insertion of numerous new technologies, to include improved unmanned aircraft systems control, cognitive decision aids, and an open systems architecture. The Marine Corps has completed fielding of the Boeing-Bell Helicopter V-22 tilt-rotor, a version of which is also employed by Air Force Special Operations Forces. The Marine Corps is also in the test phase for a new CH-53K heavy lift helicopter, which offers more power but also a fully digital cockpit, and is produced by United Technologies Corporation and Sikorsky.

For fixed wing aircraft, the Corps is the first service to operate a ver-

[52] US Dept of the Army, *Army Equipment Program in Support of President's Budget 2015*, cit.

sion of the F-35 Joint Strike Fighter (JSF). The "B" variant has a short take-off/vertical landing capability, and is projected to achieve initial operating capability in 2015. The Corps will also acquire a smaller number of "C" (carrier) variants, along with the Navy. The Air Force is buying the conventional take-off and landing "A" variant. All variants make heavy use of ICT, using networked information not only from on-board sensors and weapons but from other aircraft as well. The advances they offer in netted sensors are seen as a significant advance over current aircraft.[53] Lockheed Martin is the prime contractor for the JSF program.

Protection. In addition to the protection inherent in their manoeuvre platforms, US ground forces continue to invest in bringing greater network capabilities to other protection programs. Beyond the upgrades to the Paladin self-propelled howitzer system, the Army is improving the fire control and launcher mechanical systems for the Lockheed Martin-built Multiple Launch Rocket System (MLRS) mobile launcher. It is also continuing to procure Lockheed's TPQ-53 counterfire target acquisition radar, which utilizes networks to support remote operations.

The Marine Corps' primary program aimed at increasing protection from aerial threats is the G/ATOR, or Ground/Air Task Oriented Radar. Produced by Northrop Grumman Electronic Systems, the G/ATOR will have two blocks. The first focuses on short-range air defence, while Block 2 will focus on counter-fire targeting. Additional blocks are planned but not yet fully defined.

Beyond an array of artillery, air and missile defence programs, both the Army and Marine Corps are investing in more robust countermeasures for protection against electronic manoeuvre and attack. During the wars in Iraq and Afghanistan, much of this investment was focused on quickly enhancing and expanding the number of both passive and active jammers to prevent detonation of IEDs. All of the services, to include the ground forces, have recognized that opportunities for adversaries to exploit the electro-magnetic spectrum are in fact much broader, driven in many cases by commercial advances in ICT. To help address this challenge, the Army is looking to establish a new laboratory to test new techniques, and has been seeking solutions for a series of radio frequency-related challeng-

[53] US Marine Corps, *Concepts and Programs: Aviation, Joint Strike Fighter (JSF)*, https://marinecorpsconceptsandprograms.com/programs/aviation/joint-strike-fighter-jsf.

es.[54] All of the services are also participating in a broader Pentagon-wide effort to identify a range of new spectrum-related technologies.[55]

Sustainment. Each service also participates in the Global Command Support System (GCCS) program. GCCS is a web-enabled, real-time finance and logistics information system for units at home and when deployed, intended to provide real-time visibility into supply and maintenance needs. The prime contractor is Oracle, based in California. Another key maintenance program for the Marine Corps is the Electronic Maintenance Support System, a man-portable electronic maintenance device that can operate either networked or disconnected, and provides users with equipment interfaces, access to technical data, and reporting forms. It is developed by the Navy and GovWare LLC of Arizona.

All of the services are also focused on better leveraging ICT to enhance medical support. In addition to Defence Department-wide investments to increase access to electronic health records, some of the services are also investing in networked capabilities to streamline medical logistics and increase the amount of health information available to deployed forces.

Key enablers. Space remains one of the most crucial NEC supporting domains, and receives significant resources. As noted above, the US has multiple major satellite constellations, to include WGS (built by Boeing), SBIRS (built by Lockheed Martin and Northrop Grumman), and AEHF, also built by Lockheed Martin. DoD is also increasing the use of commercial satellites, and considering whether the US military should accept a slower evolution in the capability of each new satellite in order to reduce technical risks and lower costs.[56] Providers include Intelsat, Braxton Technologies, and DigitalGlobe, which recently merged with GeoEye.

Finally, while subject to strong budgetary pressures, all of the military services have continued to expend large amounts on ICT services. One recent report found that Army contracts for services overall fell by 15%

[54] Justin Doubleday, "Army aims to jump-start development of radio-frequency defenses", in *Inside the Army*, 29 December 2014.

[55] Scott Maucione, "Multiple DoD components have high demand for spectrum innovation," in *InsideDefense.com*, 31 December 2014, http://insidedefense.com/defensealert/multiple-dod-components-have-high-demand-spectrum-innovation.

[56] See, for example Marcus Weisgerber, "USAF General: DoD Must Change How it Buys Satellites", in *C4ISR & Networks*, 19 August 2014, http://www.c4isrnet.com/article/20140813/C4ISRNET06/308130001.

between 2009 and 2012. However, ICT services contracts declined by only 4% over the same period.[57] Most of the major US defence companies provide these services, to include Lockheed Martin, Northrop Grumman, and General Dynamics.

1.4 Future challenges

ICT and NEC are clearly here to stay for the US military, and many feel that their potential is only partially realized. However, obstacles remain. These include technical issues, still elusive interoperability, funding constraints, institutional barriers, and legal and policy issues.

Technology. Despite the dizzying pace of technological advancement, technical issues with NEC persist. Perhaps the most critical are those imposed by the basic physics of size, weight, and power, which continue to limit the full exploitation of NEC both for weapon systems and at the level of the individual service member. US ground forces remain focused on evaluating the relative benefits that inserting new NECs offer relative to their associated weight and power demands. To that end, they continue to invest in research associated with developing higher energy density and/or lower weight batteries, for example. And while cyber defence is an increasing focus, operational forces still occasionally chafe at the resulting restrictions or impediments adopting greater security entails. The tension between security and functionality continues plays out in individual programs as well. For example, the Army's version of the joint intelligence system (DCGS-A) has been very publicly criticized for failing to sufficiently leverage commercial developments. An element of the Army's response is that some commercial systems cannot adequately or securely tie to the totality of US intelligence databases and analytic networks. Nevertheless, the pressure on and within the military services is significant to on the one hand enhance efficiency and effectiveness by drawing from commercial advances to the greatest possible extent, while on the other minimize the risks of data compromise.

[57] Jesse Ellman, Gregory Sanders and Rhys McCormick, "U.S. Department of Defense Contract Spending and the Industrial Base, 2000-2013", in *CSIS Events*, 16 October 2014, http://csis.org/node/52055.

Interoperability. While interoperability – with other US services as well as with international partners – is in part a technical issue, it is also a policy one. US strategy clearly states that US operations will be joint, and also that they will be international in nature. Though every US administration has and will continue to reiterate the sovereign right to take unilateral action, it is universally accepted that US unilateral military operations are almost inconceivable. Thus interoperability continues to be a priority at multiple levels: within each military service, across the services, and with international partners. That priority is reflected in acquisition guidance as well.

While the rhetoric is strong, however, implementation continues to lag behind. Indeed, the US Army found that it was fielding so many different network-enabled systems so quickly into Iraq and Afghanistan that it lacked the requisite processes to ensure the systems were interoperable even among US Army formations.

To address this challenge the Army created the Network Integration Evaluation (NIE), an event held multiple times a year aimed at testing system interoperability within a US brigade, packaging new capabilities into planned increments, and identifying promising new technologies for more rapid deployment.[58] Though the NIE's value has been questioned both by defence suppliers and the Congress,[59] the Army maintains that it has great utility in helping the service both to evaluate possible new systems and to assess whether other processes or changes can be made to enhance the utility of existing equipment.[60] While Army leaders have been steadfast in their support for the NIE, they have clearly recognized that continued criticism threatens its viability. To that end, they are now planning to evolve the NIE into a broader "Capabilities Integration Assessment," or CIA, that will expand its mandate beyond network technologies. They also plan to tie it more directly to the Army Warfighter Assessment, which will become the primary venue for experimentation and concept

[58] US Dept of Defence, Director Operational Test and Evaluation, Army Programs, *Network Integration Evaluation (NIE)*, 2011, http://www.dote.osd.mil/pub/reports/FY2011/pdf/army/2011nie.pdf.

[59] See, for example, Ellen Mitchell, "Shyu: Army to procure $25M in technologies tested at NIE 14.1", in *Inside the Army*, 8 September 2014.

[60] Ellen Mitchell, "Key Army official predicts growth of "Network Integration Evaluation" drills", in *Inside the Army*, 3 October 2014.

development, with the CIA ultimately becoming the final testing and validation forum prior to fielding. Further, in the short term they intend to focus upcoming war games more directly on interoperability with the other US services as well as with key international partners.[61] The Army, along with all of the other US services, will also continue its participation in the annual Joint Users Interoperability Coalition Exercise (JUICE), an interoperability-focused exercise within the services, with other government agencies, and with multiple international partners. From a technical perspective, the Army is shifting some of its acquisition approaches to involve industry in discussions about how to best structure open architectures for programs such as robotics and unmanned systems,[62] a step that should improve functionality as programs evolve.

All that said, budget pressures appear to be encouraging each of the services to "start at home," placing first priority on enhancing interoperability internally, then with the other US services, and lastly multi-nationally. Each is trying to preserve its participation in international exercises to the greatest possible extent (for both military and diplomatic reasons), which will likely continue to be the main venue for working through international interoperability issues in the coming years.

With respect to acquisition policy, the Defence Department stipulates that equipment will be interoperable in general, and specifically that equipment purchased for individual operations be interoperable with all coalition partners.[63] This is amplified by additional guidance that all information technology used by any organization within the Department must interoperate "to the maximum extent practicable" with existing and planned systems, and with the equipment of other forces (to include international).[64] However, aligning investments and standards across na-

[61] These wargames may help to align concepts and intentions, but are unlikely to provide insights into actual technical capabilities. Joe Gould, "New war game to focus on tech, partnerships," in *Defense News*, 13 October 2014, http://www.defensenews.com/article/20141013/SHOWSCOUT04/310130030.

[62] Mary-Louise Hoffman, "Heidi Shyu: Army eyes interoperability, open standards for ground robotic system", in *Executive Gov*, 15 August 2014, http://www.executivegov.com/?p=62462.

[63] US Dept of Defence, Instruction 2010.06, *Materiel Interoperability and Standardization with Allies and Coalition Partners*, 29 July 2009, http://dtic.mil/whs/directives/corres/pdf/201006p.pdf.

[64] US Dept of Defence, Instruction 8330.01, *Interoperability of Information Technology*

tions continues to be a challenge. As one US Army official in Europe recently lamented, NATO countries are still unable to field radios capable of direct communications,[65] in part because alliance interoperability does not play a sufficiently prominent role in national acquisition decisions.

Operationally, even if the technology enables data sharing, approving that sharing often requires detailed bilateral negotiations that may not envision every tactical permutation, leading to continued friction during the actual conduct of operations. US defence officials are attempting to identify the kinds of agreements that might be necessary and get them negotiated prior to actual operations to help reduce these barriers, but their success remains to be seen. One perpetual point of tension internationally has been US rules on data sharing. Over a decade of operations with a wide range of partners has resulted in much greater sharing than had previously been the case, but progress has still been slower what many believe is necessary. Capabilities such as the Afghan Mission Network, which draws and shares data from national networks, have greatly enhanced multinational data sharing in that operation, but solutions remain bespoke.

Resources. While the US defence budget dwarfs almost every other nation's budget, there is a robust domestic debate around national fiscal issues in general and about the defence budget in particular. The US has exhibited a consistent pattern of defence budget growth and reduction, and many analysts expected to see the large budgetary increases of the 2000s cut back as US forces left Iraq and Afghanistan. Some analyses have made clear, however, that there have been structural changes within the defence budget that make such reductions more difficult than they have been in the past. Unlike past budgetary growth, much of the additional expense over the 2000s was not due to large numbers of additional personnel. This means that traditional practices of cutting the size of the force do not yield the same level of savings as they did in previous drawdowns. Further, in 2014 in particular, the number and diversity of national security crises – from Russian incursions into Ukraine, to the Ebola outbreak

(IT), including National Security Systems (NSS), 21 May 2014, http://dtic.mil/whs/directives/corres/pdf/833001p.pdf.

[65] Walter Piatt, "The Future of European Collective Defense", in *CSIS Events*, 16 October 2014, http://csis.org/node/52206.

in Africa, to the advance of the Islamic State in Iraq – have caused many to recalibrate expectations of any "peace dividend."[66] While the pressures on US military capabilities are growing, current law passed in 2011 still calls for capping government spending (to include defence) at rates lower than were previously planned. If the Executive Branch submits budgets above the mandated spending caps, funds in each Department (to include the Defence Department) are subject to across-the-board cuts.

The law has been controversial since its passage, and Congress and the Executive Branch have been engaged in political jockeying in an attempt to shift blame for cuts to the other branch. The practical result for the military has been not only less funding than they think they need, but also a high degree of uncertainty about what their budget levels will be going forward.[67] US ground forces have been reducing manpower as quickly as they believe is possible while still retaining the appropriate mix of experience, as well as cancelling planned procurements. The Army has adopted a strategy of incremental fielding of key capabilities such as WIN-T, which to some degree increases the interoperability challenges as units have differing versions of various types of equipment. The Marine Corps benefits from its smaller size, but also has been forced to prioritize fielding of key equipment. And both services have had to slow the advance of other ICT and NEC development and purchases. Both services maintain that further reductions may be necessary if there is no political consensus to restore funding to defence accounts.[68]

Institutional. There is a broad and decades-long consensus that US

[66] As one notable example, the editorial board of the influential newspaper *The Washington Post* called for restoring defence spending to previously planned levels. "Paying for wars against the Islamic State, Ebola, and more", in *The Washington Post*, 5 October 2014, http://wpo.st/S9aG0.

[67] This is because the Executive Branch has declined to submit budgets that comply with the statutory budget caps, in the hopes that the Congress will relax them. This strategy achieved partial success in 2013, when a bill providing some temporary (two year) relief to the budget caps was passed. But the way ahead remains uncertain. The Executive Branch continues to appear unwilling to submit budgets in compliance with mandated levels, with the Congress similarly unwilling to provide more resources. Absent another bipartisan agreement to provide relief, Defence Department accounts will again be subject to percentage-based reductions in the coming fiscal year.

[68] Jason Sherman, "In event of sequester, entire modernization portfolio to be 'stretched out'", in *InsideDefense.com*, 14 October 2014.

processes for acquiring military goods and services is highly problematic. How best to change the existing system is much more contentious, however, and so it persists. There have been dozens of reports, commissions, and studies conducted on "acquisition reform," with little demonstrable progress. Both the Defence Department and the Congress are currently engaged in yet another spate of activity designed to produce change, though optimism about their ultimate success is by no means universally shared. Nevertheless, one of the key themes in the latest round of the acquisition reform debate is the need for the Defence Department to embrace a more nuanced, less "one-size-fits-all" approach to buying different kinds of military capabilities. In the NEC context specifically, some have suggested that the traditional acquisition system might be suitable for fixed networks, for example, but that a faster, less rigid system is needed for other ICT and related services.[69]

The idea is not new. In general, when applied to ICT purchases, existing processes are broadly seen to create delay, a failure to include the most advanced capabilities, and unnecessary costs. Yet the proposed solutions vary. In a 2009 report, the influential Defence Science Board (DSB), an advisory group to the Secretary of Defence, found that the fundamental problem the Department of Defence faces is that "the deliberate process through which weapon systems and information technology are acquired by DoD cannot keep pace with the speed at which new [IT] capabilities are being introduced in today's information age." Consequently, the Department needs a new acquisition system for information technology.[70] Others argue that the current system is viable if implemented differently. For example, some research centres have published guides aimed at helping Pentagon buyers to improve their agile acquisition practices.[71]

Acknowledging these challenges, senior Defence officials have adopted the latter approach, pledging to better utilize existing processes rather

[69] See, for example, Justin Doubleday, "Army crafting career field, occupational specialty for cyber forces", in *Inside the Army*, 19 September 2014.

[70] US Dept of Defence, *Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology*, March 2009, p. 1 and 4, http://www.acq.osd.mil/dsb/reports/ADA498375.pdf.

[71] Pete Modigliani and Su Chang, *Defense Agile Acquisition Guide. Tailoring DoD IT Acquisition Program Structures and Processes to Rapidly Deliver Capabilities*, Mitre Corporation, March 2014, http://www.mitre.org/node/18951.

than reinvent them. To that end, the Joint Staff recently modified the official acquisition system to create a new category for information technology programs, allowing greater delegation of decision authorities. The Pentagon is also attempting to recruit acquisition professionals with the requisite knowledge of IT systems.[72] How well these efforts will succeed, however, is not yet known, and some experts maintain that an entirely different process will ultimately be necessary. And Congress has yet to weigh in with its view. Industry is watching closely to see whether promised legislative reforms in 2015 will address this topic. If they do, it is still unclear whether Congress would propose a new system for ICT, modify the existing one, some combination of the two.

One of the reasons that the Defence Department has had difficulty relying more heavily on commercial ICT developments is that it is accustomed to being a market driver as opposed to a market taker. Defence officials have traditionally asked companies to make the necessary changes to meet military needs (e.g., to increase security features, or to enhance a given piece of equipment's ability to withstand temperature or other weather extremes). But for many ITC suppliers, the military market is so small relative to commercial alternatives that entering it is not worth the trouble, and investing in modifications is inefficient. The task then falls to more traditional defence companies, frequently adding time and significant expense or taking away key functionalities, which cuts against some of the core rationales for buying commercially-based products in the first place.

Intellectual property (IP) rights are another key sticking point. The Defence Department has been increasingly vocal about its intent to move away from buying systems with proprietary hard- and software interfaces, a desire reinforced by the Congress.[73] However, companies that have business models structured around long-held IP are loathe to move to more open architectures, particularly when they perceive that time is on their side. Companies that have developed key parts of major systems

[72] US Senate, Committee on Armed Services, *Testimony of Frank Kendall*, 30 April 2014, http://www.armed-services.senate.gov/imo/media/doc/Kendall_04-30-14.pdf.

[73] For example, the Fiscal Year 2013 National Defence Authorization Act included a provision that prohibits the Defence Department from buying proprietary or undocumented waveforms or interfaces.

that are aging and need replacements or upgrades have to decide whether they want to continue to compete to play a possibly lesser role going forward. Some are making that choice, but others know that finding an alternative solution that would provide equivalent levels of interoperability or performance would be cost-prohibitive for the military services, so they continue to market proprietary solutions. Another more practical obstacle results from the time it takes to develop the standards sufficient to support an open-architecture approach. In cases where they have not yet been established, senior leaders have been forced to waive legal requirements for non-proprietary solutions to move ahead with necessary purchases.[74]

Though the path is long, the military services continue to make steps to better support the leveraging of commercial developments. This depends on the details of IP and contracting, but also extends to other processes like planning and budgeting. For example, the Defence Department is currently considering how best to modify how it assesses its future needs for commercial satellite support in order to support more efficient purchasing practices.[75]

Conceptual. As is discussed above, the services, and the Defence Department more broadly, all recognize the twin opportunities and vulnerabilities associated with high levels of network reliance. However, at present there is no clear consensus about how best to address the vulnerabilities. The natural predilection of the military services has been to defend, especially in the cyber arena – to increase spending on cyber defence forces, network infrastructure and design, and other key defence approaches. In space, that approach has given way to a more balanced focus on increasing both defence and resilience, for individual payloads and satellites and across constellations. In the broader electro-magnetic spectrum context, the strong focus on defence is to some degree augmented by a (culturally weaker) strain of offense borne out of the electronic warfare tradition. Some of these approaches are based in how the threats have evolved, and have cultural and bureaucratic roots. Others reflect the actual nature of

[74] Jordana Mishory, "DoD waives data link requirement so Navy can obtain eight systems", in *Inside the Pentagon*, 14 August 2014.

[75] Scott Maucione, "Pentagon eyes reforms in commercial SATCOM acquisition practices", in *Inside the Pentagon*, 9 October 2014.

the challenge, as well as the costs (both financial and otherwise) of alternative solutions. But there has yet to be a robust national conversation about the best strategy across all aspects of the NEC challenge, and thus whether additional change is needed. For example, the Commander of US Army Cyber Command has suggested that total cyber defence is not possible, and that the Army has "to be able to operate while compromised."[76] The ability of US ground forces to train this way is challenged by a number of factors, from domestic laws that restrict certain kinds of cyber activities within the United States to insufficient resources to support such training. But it may also be a reflection of the desire to wish the problem away; it is far less complicated to assume the networks, somehow, some way, will be functional.

Legal/policy issues. Finally, as is frequently the case, ICT developments in many instances move faster than do the policies and legal structures that would enable their full employment. The specific challenges associated with interoperability have been discussed above, but the problems extend to other areas as well. For example, in a US-specific context, policies governing the military services' use of cloud technologies reflect some of the tensions between security concerns, affordability, and interoperability. The Defence Department's Chief Information Officer recently acknowledged that her office has been too slow to issue guidance about how each of the services procure cloud-based services. Ultimately, DoD decided upon a decentralized approach that allows each to independently buy digital cloud systems if those systems comply with common standards. However, this immediately raised concerns that interoperability could be comprised, either now or in the future as providers improve their offerings.[77] While such fears may prove unwarranted, they remain representative of the challenges that persist to obtaining systems and services that allow for true interoperability among organizations, US or otherwise.

Another area in which technological advances are eclipsing the existing legal structure is with respect to military activities in the electromag-

[76] Edward C. Cardon, *Keynote Address*, Brookings Fifth Annual Military and Federal Research Symposium: "Securing America's Future in the New 'Interwar Years'", 12 March 2014, http://brook.gs/1F8BpAi.

[77] Scott Maucione, "Upcoming DoD CIO cloud policy leaves questions over interoperability", in *Inside the Pentagon*, 9 October 2014.

netic spectrum. As new capabilities are developed, many seek to integrate intelligence information with the ability to deliver effects. This possibility creates an inherent tension between Title 50 of US Code, which governs intelligence activities, with Title 10, which governs military operations.[78] Electronic warfare has been conducted under Title 10 authorities, but the ability to marry electronic warfare activities that seek to disrupt signals with cyber operations that might seek to affect the information within those signals, for example, presents new legal challenges that have not yet been fully examined, let alone resolved.[79] These are further complicated by laws restricting what can be done within the United States, which affects how the military can train to employ such tools.

1.5 Conclusions

In sum, US ground forces and their sister services are and will continue to be fully reliant on NEC, in every warfighting function and in every warfighting domain: air, land, maritime, space and cyber. The degree to which NEC is used for offensive and defensive purposes varies in each domain and function, as does the balance between a defensive versus dispersed approach to mitigating associated vulnerabilities. And while ICT and NEC have changed the way Americans do and will fight wars (and all other military missions), multiple obstacles to leveraging them still further remain. Nevertheless, the ICT/NEC bell has been rung; the challenge for the US Army and Marine Corps will be to maximize its benefit while minimizing its risks.

[78] Sydney J. Freedberg, "STRATCOM lacks authority, $$ on electronic warfare", in *Breaking Defense*, 7 October 2014, http://breakingdefense.com/?p=16291.

[79] Maren Leed, *Offensive Cyber Capabilities at the Operational Level. The Way Ahead*, Washington, Center for Strategic and International Studies (CSIS), September 2013, http://csis.org/node/46679.

2.

The Paths towards NEC: France, Germany and the United Kingdom

Nick Brown

2.1 Introduction

France, Germany and the United Kingdom are all well on their ways towards military digitization and the ability to field a truly Network Enabled Capability (NEC).

At a national strategic level, all three countries appear to have each taken a slightly different path. In some ways, the countries' experience with their individual soldier digitization programs provide a metaphor for their wider experience. For example, France's early adoption and commitment to its FELIN digital soldier ensemble and its relatively late deployment into Afghanistan enabled the country to develop a cohesive package of systems that worked together at an individual level and provided the building blocks to expand that to wider platforms on the battlefield. By comparison, the UK's similar FIST aspirations provided some initial successes, but the country's adoption of Urgent Operational Requirements (UORs) – acquisitions of systems such as radios, electro-optical sights and other systems off-the-shelf from a range of suppliers to get them into soldiers' hands as soon as possible – may in retrospect have imposed unintended limitations that eventually derailed FIST and other projects. By definition, this reactionary acquisitions process prevented the MoD from acquiring or developing elements and modules that would work together as a cohesive system.

In a similar vein, the British Army's plans for a straightforward, phased roll out of enhancements to its Bowman communications architecture were hijacked by the need to balance getting the latest equipment standards out to theatre as soon as possible, while ensuring that the troops heading out on the next rotation had access to – and were certified to use – those systems too. In a peacetime situation, that wouldn't have been a problem, different standards could be phased in and out by a company or regiment at a time as they became available, but operational rotations for Afghanistan and Iraq proved a complication too far. The army has learnt from that experience and is attempting to ensure that it won't happen again with the new system currently in development to take the army beyond Bowman.

The British Army's experience with a single prime contractor – General Dynamics – for the Bowman project has also prompted it to take a completely different approach to the Project Morpheus work to replace it. Instead of giving a "big bang" contract to one supplier, the army's current plan is to hold a series of competitions to deliver distinct components in a coherent manner. Although this requires the army to generate and sustain a new degree of expertise in house to manage the project, it leaves the project less hostage to the whims and controls of a single contract "owner."

Germany's experience with its IdZ ensemble is somewhere between the two, having stuck to its original plans and concept in principle unlike the UK, but being more flexible than France and not being afraid to junk the elements that didn't work as hoped for and looking for workarounds.

Generally speaking, despite sharing an appreciation of modern operational realities garnered from fighting alongside each other in Afghanistan and other theatres so far this century, each country remains very much focused on trying to correctly harness the potential benefits of NEC at a national service or joint level.

An argument can be made that this is the most sensible approach – there is little point in establishing an assured means of networking with international allies if the military building blocks at the squad or national joint task force can't be made to work closely together. But it remains a fact that one of the biggest challenges encountered for combined operations in Afghanistan/Iraq/Libya and elsewhere was the ability to mesh together international forces that deployed with independent interpretations of NEC concepts and systems.

Compatibility was – and still is – an issue at the national level. France, Germany and the UK are all working to remove roadblocks their own systems, but there is little more than lip service to getting their networked systems to talk to each other across national borders. Much of the connectivity achieved on operations and training exercises to date has remained "swivel chair" networking. That is to say that individual systems can be made interoperable by adding a human in the loop, sometimes using different systems and physically switching between the two.

The danger is that in the absence of agreed standards and architectures, countries are running a very real risk that even though they are working to ensure their own connectivity, they are still doing so in an individualist manner. As such, it is far from certain that future coalition operations will not encounter a familiar lack of coherence, which prevents a combined force from truly being able to exploit all of the benefits of NEC. This is despite the increasing prevalence of commercial network integration laboratories that can be used to test the ability of systems to interface smoothly ahead of deployment. In an era where unilateral military operations are becoming increasingly hard to imagine, this is a hard position to reconcile.

Recent air operations have provided a fig leaf of respectability to multi-national net-centricity, because the near universality of strike aircraft access to Link 16 and unified radio technologies and procedures have enabled air forces to at least appear to be working seamlessly together. Indeed, at a basic operational level, there is a wealth of data that proves air forces can work together to get ordnance onto target. The real question is whether any given weapons release has been enabled and truly optimized by that networked capability or whether the network has just provided a framework to act within.

Operations over Libya would tend to add weight to that latter argument. The lack of truly networked, multinational timely targeting meant that ground targets were needlessly attacked and re-attacked despite having been knocked out hours or – in some cases – days previously. French navy assets were so frustrated by this that they began to conduct their own time-sensitive targeting by rapidly networking reconnaissance from the Damocles targeting pods carried by returning Rafale and Super Etendards back to the carrier, where a team assessed likely targets and transmitted their coordinates to outgoing strike packages. As impressive as this was at a national level, in some ways it likely added to the issue as French assets were acting within their own network loop and on several occasions, UK Royal Air Force Tornados and even French Air Force Mirages ended up flying pointless sorties.

There is, however, some potential that this picture will improve in future. There is growing appreciation of – and support for – open architectures and agreed interface standards between France, Germany and the UK at some levels. For example, the UK's Generic Vehicle Architecture is showing signs of being adopted as a European and NATO standard.

Even so, it does not appear that there is much appetite for joint multinational procurement cooperation and the history of European attempts to develop and jointly procure everything from rifles to fighter aircraft is littered with more failures than successes. Satellite communications should show great potential, but that seems to be perpetually impossible to reconcile between France, Germany and the UK.

At another level, the borderless nature of the cyber realm may prompt some degree of collaboration and cooperation, certainly at an information-sharing and criminal level, but for now it seems that France, Germany and the UK are likely to retain control and independence at a national level.

Similarly, a lack of coherence on radio and data interfaces is proving a challenge as these three countries look to their requirements for the coming decade. It would seem that the cooperative spirit is strong, but the body is weak.

2.2 Cyber

2.2.1 United Kingdom

The UK defence establishment's relationship with cyber was set out in the 2010 Strategic Defence and Security Review (SDSR) and the national approach has made some strides towards these aspirations over the last five years.

Specifically, the 2010 SDSR stated that

> We will establish a transformative national programme to protect ourselves in cyber space. Over the last decade the threat to national security and prosperity from cyber attacks has increased exponentially. Over the decades ahead this trend is likely to continue to increase in scale and sophistication, with enormous implications for the nature of modern conflict.[1]

A new strategic defence review is scheduled to be released later in 2015, which may shift the emphasis slightly, but it is expected to be framed within the context described in 2010.

Under this overarching concept, the MoD signed up a number of commercial companies to secure its own networks and then, by extension, those of garrison and deployed forces.

The latter is an interesting development, as up to that point the British armed forces, like most of their contemporaries, had in public at least prided themselves that their communications and computer systems were inherently secure. After all, they had been developed to withstand the subtly different offensive attentions of electronic warfare.

For the most part, that security remains true for systems at the tactical edge. However, the MoD realized that the ubiquity of portable computers – personal and work – wireless networks, USB and other standard interfaces, software-defined radios and the increasing adoption of commercially sourced operating systems for military systems were becoming impossible to police in the traditional manner and rendered unacceptable vulnerabilities. By 2010 the concept of cyber defence was uncontroversial and had generally been accepted as necessary, but that meant that cyber operations were inherently reactive, officially leaving the initiative to "rogue" states or non-state hacker groups and criminal organizations.

In an attempt to wrest this back, the UK became one of the first countries to tacitly acknowledge that it possessed national offensive cyber capabilities when, in September 2013, Defence Secretary Philip Hammond stated that the UK was "developing a full-spectrum military cyber capability, including a strike capability."[2]

[1] UK Government, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, 19 October 2010, p. 4, https://www.gov.uk/government/publications/the-strategic-defence-and-security-review-securing-britain-in-an-age-of-uncertainty.

[2] UK Ministry of Defence Joint Forces Command and Philip Hammond, *New cyber*

One of the biggest steps to be made to this end was the establishment in May 2013 of the Joint Forces Cyber Group. Hammond also announced in September 2013 that this force was to be bolstered with the activation of a new cyber reserve force – essentially an arm of the part-time Territorial Army envisaged to be made up of several hundred nationally minded IT professionals and hackers – to react to cyber offensives.

As of early 2015, it is unclear how successful that recruitment drive has been. The MoD declines to detail either force and, despite Hammond's candour, is perpetually sensitive about the cyber capabilities resident within the armed forces. As such, its exact capabilities remain shrouded in secrecy.

Likewise, the Government Communications Headquarters (GCHQ) organization is understood to have substantial cyber capabilities, but the details are hedged around and protected by official secrecy and the capabilities, requirements and technologies used are all considered very sensitive.

GCHQ does periodically break cover in the cyber domain, however. In August 2014, for example, it accredited six universities to teach postgraduate Masters Degrees in cyber security. Later that same month, it enlisted the power of crowd sourcing by launching an online game testing players' abilities to protect a fictional aerospace company. However, this was more of a recruitment and assessment tool and offered little insight into the organization's capabilities.

Marginally less sensitive, but still not comfortably discussed in the public arena, are the details of arrangements set up under the Defence Cyber Protection Partnership (DCPP). This saw the MoD and GCHQ team up with BAE Systems, communications giant BT, Cassidian (now part of Airbus Defence and Security) and Lockheed Martin to share concerns and responses to cyber attacks.

The former Cassidian plays a strong part, providing network security services to the MoD through its facility in south Wales, including deployed forces under a recent development. The latter was included in a 2014 urgent operational requirement to add secure, but unfettered internet access to the UK's TACIP network nodes deployed to the Persian Gulf.

According to Steve Whitby, Airbus Defence and Security's strategic accounts director, TACIP operators were limited to accessing military com-

reserve unit created, 29 September 2013, https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit.

munications bearers, but can now access the internet through the MoD Defence Information Infrastructure portal with a direct link back to the Wales facility.[3]

In theory there is a large degree of scope at a national level for the UK to cooperate internationally in the vexed field of cyber defence, particularly through NATO, but there is little in the public domain giving any concrete indication that the UK is actively looking beyond its national capabilities from a military perspective. Like other nationally vital aspects of defence, the UK shows a strong inclination to retain a sovereign capability. Indeed, perhaps more than some other areas where the erection of "Chinese walls" provide sufficient security, the insidious and all-pervasive nature of computer networks means that cyber security is often treated in a similar vein to espionage and the need to keep it clandestine.

Industry is a different matter, with many of the large, multinational defence industry primes – Airbus, BAE Systems, Thales, Lockheed Martin, Northrop Grumman and Raytheon – already engaged in the field. All of them claim varying degrees of cross-border reachback and capability. Of particular note to this report, Airbus has its main centre of gravity in the cyber field with Cyber Security Customer Solutions Centres in France, Germany and the UK.

2.2.2 France

Like Germany and the UK, France has taken the cyber threat very seriously and also explicitly claims the ability to undertake offensive cyber operations.

Dedicated resources have been steadily ramping up and on 21 January 2015, Defence Minister Jean-Yves Le Drian announced that the Ministry of Defence had specifically allocated 1 billion euros of funding to boost the country's cyber security. That money will be disbursed to the Centre d'analyses en lutte informatique defensive (CALID – Centre for the Analysis of Information Defence) body and the DGA, both of which are planning for radical expansion.

CALID will remain relatively small, but intends to grow its staff from 20 in 2011 to 120 by 2019, while the DGA's cyber staff team at the Bruz-

[3] Nick Brown, "Airbus adds internet freedom to UK TACIP", in *Jane's International Defence Review*, 26 November 2014.

based information superiority centre is set to rise from 250 to 450 in "the next few years."

The new money will also help to establish a formal cyber operations centre of excellence in Rennes, triple the number of upstream cyber defence studies and broaden the current network of 80 cyber defence reservists – the French equivalent of the UK's Joint Force Cyber (Reserve) – that was first stood up in 2012. The concept for the latter envisages using the group to respond to emerging crises, but Le Drian also noted that he wanted to create an operational force of cyber defence specialists, which would presumably be more proactive.

Cyber defence has been a key element of French defence thinking since its 2013 defence White Paper, but rationalizing all of this investment, in late January, Le Drian told the International Forum on Cyber Security in Lille that cyber operations have become a "national priority."

According to Major Arnaud Le Dez, deputy head of the "preparedness" branch of CALID, the Ministry of Defence suffered 700 cyber incidents – ranging from relatively innocuous viruses that might be experienced by any enterprise right up to serious attempts to tackle the ministry's networks – in 2013, which represents a fourfold increase since 2011.[4]

As with the UK, France has contracted Airbus Defence and Space to help with its network security. Part of the French interest has seen the company acquire the company's Cymerius network monitoring tool. This scans networks, looking for anomalies and suspicious activity, but is a decision-assistance tool rather than a full defensive suite. It is currently being used at the ministry and versions are being deployed into French Navy ships as an integral part of their upgrade to the Rifan 2 IP-based communications system.

Although not specifically a military application, another recent area of cyber interest occurred in October 2014, when the GICAT French defence industry trade association signed an agreement with cyber security specialist group Hexatrust to develop the structure of the national cyber security market.

Hexatrust is a kind of trade organization group, tying up 18 information and cyber security companies. The strategy of the GICAT deal is to

[4] Nadia Deseilligny, "France earmarks EUR1 billion in spending on cyber defence", in *Jane's Defence Industry*, Vol. 31, No. 2 (1 February 2014).

promote French-developed cyber solutions nationally and around the rest of the world to the exclusion of other European options, so although there is potential for collaboration France would not appear to be wholly open for international business. Or if it is open, then international companies can expect hard fought competition from local industry.

There is also significant cyber capability resident within the larger French national and multi-national industry. One of the more substantial recent industrial machinations included Thales' acquisition of Alcatel-Lucent's cyber and communications security business in October 2014.

2.2.3 Germany

Germany has been a little slower to address the cyber threat than France and the UK, possibly as a result of an institutional resistance to "snooping" in the shadow of decades being watched by the Stasi and a national desire to reconcile governmental transparency with personal privacy.

Nevertheless, in 2010 Germany set up a National Cyberdefence Centre to coordinate resources and pool the various military and government stakeholders. Over the last couple of years it has accelerated development and joined the ranks of the countries claiming an offensive capability. In some ways, this policy is perhaps unexpectedly forthright for a country that has only recently deployed its forces out of area – and even then mostly on peacekeeping tasks – and imposes more restrictive controls on arms transfers than most of its peers.

However, concern about the rise in attacks appears to have risen in the last few years. Incidences such as the high profile hacking of Angela Merkel's telephone in 2014 and then early January 2015 cyber attacks on government websites from pro-Russian hackers protesting Germany's position on Ukraine helped prompt Germany to intensify its position on cyber defence. In particular, Germany is working to establish an early warning capability looking to pre-empt, disrupt and prepare for potential cyber attacks under the Bundesnachrichtendienst (BND) foreign intelligence service's Strategic Technology Initiative.

This has attracted 300 million euros of funding between 2015 and 2020, which – although substantial – nevertheless pales next to the sums allocated by France and the UK. As the BND is purely external, it would appear that the new system is limited to seeking triggers of external threats.

The ruling CDU/CSU political coalition has adopted a formal stance that it will not take a blanket approach to electronic surveillance, but that may change at the next election of course. Meanwhile, in late 2014, the Financial Times and others quoted Stephan Mayer, a spokesman for the coalition, as saying that "There is a general view in the US that everything can be done that is technologically possible. We don't share this view. But neither should we be blind."[5]

Internal surveillance by the state is tightly controlled constitutionally, which restricts Germany's abilities in the cyber world. Nevertheless, the Ministry of Interior – Bundesministerium des Innern (BMI) – has crafted a Cyber Security Strategy framework within which to operate. This asserts that "Ensuring cyber security has thus turned into a central challenge for the state, business and society both at national and international level," but adds that the scale of the challenge is daunting: "In view of technologically sophisticated malware the possibilities of responding to and retracing an attack are rather limited."[6]

It is also explicit that the BMI's Cyber Security Strategy mainly focuses on civilian approaches and measures. They are complemented by measures taken by the Bundeswehr to protect its capabilities and measures based on mandates to make cyber security a part of Germany's preventive security strategy. Given the global nature of ICT, international coordination and appropriate networks focusing on foreign and security policy aspects are indispensable. This includes cooperation not only in the United Nations, but also in the EU, the Council of Europe, NATO, the G8, the OSCE and other multinational organizations."[7]

It is unclear exactly what measures the Bundeswehr has to call upon, but the force has a Computer Network Operations team of hackers resident within the relatively new Strategic Reconnaissance Command. It is, however, clear from this statement that Germany is a keen proponent of international cooperation at a governmental and organizational level.

[5] Stefan Wagstyl, "Germany plans early-warning defence against cyber attacks", in *Financial Times*, 10 November 2014, http://on.ft.com/1uXsbBS.

[6] German Ministry of Interior, *Cyber Security Strategy for Germany*, February 2011, p. 2 and 3, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf.

[7] Ibid., p. 5.

However, this is somewhat at odds with its approach to industry, which is more akin to that of France and the UK, with a formal policy of favouring domestic industry for its cyber capabilities.

2.2.4 EDA and NATO frameworks

The European Defence Agency has repeatedly exhorted its members to cooperate on cyber security (and other areas) but has struggled to get any traction, with virtually nothing to tangible to show for its efforts.

NATO has gained more ground, as might be expected, but Jamie Shea – NATO's spokesman during Kosovo operations, but now the alliance's deputy assistant secretary general for emerging security challenges, essentially NATO's top cyber security official – told a September 2014 cyber intelligence conference in Brussels that more needs to be done.

Although the NATO Computer Incident Response Capability (NCIRC) finally achieved full operational capability in early 2014, he said that NATO members need to simplify networks to minimize the risk of cyber incursions. "We now need to simplify our cyber structures. We've layered on so many things [to legacy systems] that there are many attack levels across our networks."[8]

As an indicator of the scale of the problem, Shea said that NCIRC had noted 200 million incidents on NATO networks everyday and 2,500 significant assaults in 2013.

But if anything the evidence of France, Germany and the UK appears to show that the number and complexity of networks and communications is growing if anything.

2.3 Command and Control (C2)

2.3.1 United Kingdom

The UK has a bewildering array of layered communications and C2 systems, with British infrastructure programs mostly named after birds.

[8] Brooks Tigner, "NATO urged to embed cyber defence into mission planning", in *Jane's Defence Weekly*, 23 September 2014.

There is some coherence and logic, but anomalies still remain in the joint realm, creating some disconnects.

For example, NATO's exercise "ARRCade Fusion" in November 2014 illustrated the British Army's adoption of the Magpie infrastructure operated by 22 Signal Regiment and this extended a communications backbone for a host of NATO players (including German and French operators). This provided satellite connectivity to Italy with a Skylark detachment (consisting of two UK/TSC 729 Rockwell Collins CCT 120 terminals operating over Skynet 5). Joint Terminal Attack Controllers joined the exercise using the Royal Air Force's (RAF) Magpie capability hard-wired into the RAF's High Wycombe complex, but the Royal Navy was left outside.

For ARRCade Fusion 14 part of the internal network in the HQ was provided using infrastructure from the new Falcon area communications system.

The next step beyond Magpie is Project Jackdaw, which will introduce a common architecture integrating Magpie. In the meantime, the UK relied on the Overtask network for operations in Afghanistan and the Defence Information Infrastructure – Land Deployable (DII – LD) providing NATO Functional Area Services and an Enterprise Services Bus to provide a common platform and common applications. This is a "mission-configurable" system meeting the requirements for NATO's Federated Mission Network (FMN) standards that will govern NATO networks in the future.

Jackdaw is expected to enter service from 2015. The main C2 application used in the HQ is the Integrated Command and Control (ICC) tool. This provides the common operational picture (COP), and can also be used to display the Recognised Air Picture (RAP) and Recognised Maritime Picture (RMP), provided by the AOC and the maritime Task Group respectively. The JCHAT facility is also a key tool, available across all components when connectivity allows.

This works well between army and air assets, but navy integration is a missing element. In general, maritime platforms with SATCOM provisions use the NATO secret Wide Area Network and have access to ICC, enabling naval crews to join in over JCHAT.

However, operational exigencies mean that there will be times when connectivity with vessels is limited to High Frequency (HF) radio, greatly reducing bandwidth connectivity between shore and ships. As a result, naval assets continue to insist on contacts using basic formal messaging traffic protocols, but the advent of far more capable systems ashore mean that land and air assets have long since dropped it, with commensurate skill fade and frustration.

Although HF transmissions can carry email, it is not formally recognised as recorded traffic and delivery is not guaranteed, so it does not have the same non-repudiation status of formal messaging, or even JCHAT, where all communications exchanges are recorded on the network's server.

At a single service level, this is of course less of an issue, but it complicates common picture establishment and creates a jarring disconnect when dealing with naval assets.

Staying within air-land C2, the British Army certified its Lockheed Martin-developed Land Environment Air Picture Provision (LEAPP) as operationally capable in December 2014. This provides a common air picture using the associated Saab Giraffe radar and Link 16. The latter inherently eases connectivity with air assets as most NATO (including French, German and UK fighters) are now suitably outfitted.

The British Army is already looking to upgrade elements of LEAPP and add new capabilities through its support contract with Lockheed Martin UK.

By far the biggest project within UK military communications is the imminent replacement for the General Dynamics UK Bowman tactical communications architecture.

Bowman itself still feels relatively new, having only finally been rolled out across the UK's armed forces in 2008, and it bears rehearsing some of the details of the in-service system as experience with it underpins the plans to replace it.

Bowman embodied the British Army's first attempt at digital communications and – as might be expected for such a game changing application of technologies – suffered significant and protracted issues in its roll out. Some of those were related to the technologies involved and others were more programmatic in nature.

Nevertheless, in its latest Bowman and ComBAT and Information and Platform (BCIP) configurations – BCIP 5.5, released in 2013 and scheduled to complete fielding in April 2015 – and various Battlefield Information System Applications (BISA), it has evolved into a very capable system.

Although headed up by General Dynamics UK, there was widespread industry support with elements provided by BAE Systems, Blazepoint, Cogent Defence Systems (now subsumed into Airbus Defence & Space), DRS Tactical Systems, Harris, ITT (now Exelis), L-3 Communications, Selex-Finmeccanica and Thales, along with integration and platform installation work at a variety of sites. The important thing to note is that it was very much a UK system and despite several of the companies involved being multinationals, it was their UK footprint that took the strain for the project.

Versions are now carried by dismounted infantry and integrated into all army platforms from the humblest Land Rover up to the Challenger 2 main battle tank, along with army and RAF Chinook, Merlin, Lynx and Apache helicopters. The Royal Navy's major surface fleet has also been outfitted.

The range of equipment associated with Bowman varies depending on role, but the base capabilities offered comprise encrypted voice and data using software-defined, frequency-hopping UHF and VHF radio sets in handheld and vehicular forms, with a UHF High Capacity Data Radio (HCDR) MANET radio providing powerful modem and self-managing mobile internet access at the top end.

An early component that ended up being acquired separately from the full Bowman project (to get it into service quickly) was Selex-Finmeccanica's UHF H4855 Personal Role Radio (PRR), which provided a building block for all future soldier digitization packages.

Although being quite a simple voice-only package, it connected every soldier for the first time with better communications than shouting and hand signals. As such, it proved a very successful acquisition that provided a paradigm shift in connectivity at the squad level and enabled the British Army to revolutionize its small unit tactics. Other armies saw the benefits and swiftly followed suit.

The UK plans to continue using Bowman for the next few years, but is planning to deliver a step change in capability from around 2018, with a comprehensive new architecture being developed under the Land Environment Tactical Communications and Information System (LE TacCIS) program, also variously known as Morpheus, and potential transition into yet another name: Battlefield Tactical Communications and Information System (BatCIS).

Interestingly, LE TacCIS covers the support of legacy Bowman and also its replacement, illustrating that the UK aims to make more of a streamlined transition than Bowman's troubled roll out. This process aims to draw together all of the elements of Bowman in a more cohesively integrated whole and add some new capabilities based one more modern technologies. In particular, the legacy Bowman waveform and architecture was not designed to be interoperable with other nations' communications systems and as the UK's forces are shrinking and it becomes increasingly likely that the UK will operate with other nations, that it more important than ever.

The MoD has aspirations that this system will be more flexible and able to remain current with technology updates as they become available and is conducting a three-stage assessment phase.

The initial phase (AP1) kicked off in 2013 with 50 million pounds in funding and is currently underway refining requirements and setting out the business case. Being used by all three services, it is notionally being conducted by the UK Joint Forces Command, but is being led by the army as the main user.

As might be expected, the project is looking closely at lessons learned from Iraq and Afghanistan, and whether those lessons might apply to future conflicts or were actually specific to those theatres. For example, ISAF's complete dominance of the communications environment enabled relatively simple and guaranteed access to high datarates, which may not be possible in a more contested battlespace, so can datarates for future systems be throttled and still meet requirements?

Forces in Afghanistan in particular got very used to full motion video – downlinked from manned and unmanned aircraft, or shared from forward-deployed units – and the MoD is assessing its value, along with where it can be best applied as essential, rather than just desirable, if the data capacity is limited. The assumption being that not every soldier in the front line or every staff officer in a headquarters area necessarily needs it.

In the meantime, one of the first concrete steps will see the development of a BCIP5.6+ for fielding in 2017. According to Colonel Richard

Spencer, head of the UK MoD's BatCIS delivery team, this could be a sufficiently improved capability to warrant a rebranding away from Bowman. Either way, the current iteration of Bowman is likely to be the last, so the upgrade of legacy vehicles will be decided by the direction of the LE TacCIS/Morpheus project.

Amongst other enhancements, this will finally enable the exploitation of the latent positioning capability inherent within the Harris PRC-152 radio, allowing others on the BCIP network to "see" the radio and vice versa, meaning that the system could finally be used for blue force tracking. (The legacy system has built-in positioning, but only at the soldier level as a location aid.)

This is likely to feed into (yet another) distinct program within the LE TacCIS project, Dismounted Situational Awareness that will provide full force visibility to army, RAF and Royal Navy assets.

> We would like to get to a point," Col Spencer told IHS Jane's Defence Weekly in mid 2014 "where, instead of a situation where Combat does everything, we have a number of smaller applications doing specifics, underpinned by some common services such as the geographic information system [GIS].[9]

LE TacCIS is understood to be looking at three options for how to fund and field these capabilities under AP1.

The first is to keep running the legacy systems for as long as possible, retrofitting patches to add capability. However, the radio technologies at the heart of the system are essentially technology from the beginning of the century and will become increasingly obsolescent, with a risk that they will be unsustainable around the end of this decade.

The second option is a hybrid approach, assessing which elements can be sensibly be retained and acquiring some new systems to ameliorate obsolescence, and the third is the most expensive up front: buying an all new architecture. The benefit of the latter is that it is more flexible, current and may be cheaper to support long term.

Whichever option the team eventually decides, it is clear that the army

[9] Giles Ebbutt, "Beyond Bowman", in *Jane's Defence Weekly*, Vol. 51, No. 26 (25 June 2014), p. 28-31.

does not want to replicate the legacy situation where the army does not own the data standards used by Bowman. According to Colonel Giles Ebbutt, editor of IHS Jane's C4I,

> this has resource implications. There is no in-house expertise within the British Army to do this at present, so assistance would be required to help integrate third-party products into a network. Resources would be required both to buy in this expertise and to grow it in-house.[10]

As such, the army would ideally like to just adopt internationally agreed standards (applying its own encryption and security over the top, of course) that would be easier to control, open up the market for new software "apps" and reduce costs through competition, as well as easing interoperability with other countries' forces.

The challenge is that the available options are still a bit of a gamble as the existing Multilateral Interoperability Program (MIP) standards vary between operators. For example, MIP Block 2 is used by France and the US – the UK's geographically and spiritually closest allies – which would appear to make it a no-brainer. However, the next tier, MIP Block 3 is used by Germany and is not backwards compatible with Block 2. Complicating things further, there are different iterations of Block 3.

So, the UK could go alone and adopt a bespoke path or create another MIP Block, but that is dangerous as it could lead to a similar situation that the UK is currently in.

An industry party is set to be contracted to investigate these standardised options as part of AP1 and should report back by the end of 2015. The whole of AP1 is scheduled to be completed by early 2016, setting the tone for the next decade's worth of UK battlefield connectivity.

The Morpheus project team must also remain cognizant of another layer of compatibility, ensuring that it can work within the Land Open Systems Architecture (LOSA), which defines "open" network interface standards under the Generic Soldier Architecture (GSA), Generic Vehicle Architecture (GVA) and Generic Base Architecture (GBA) nomenclature. GVA is probably the most advanced, with installations in the Foxhound

[10] Ibid.

vehicle, and mandated for the Warrior, Specialist Vehicle Scout and Challenger. It has proven successful so far, providing developers with agreed and formalized standards for data sharing and easing connectivity within and between vehicles.

The British Army's vehicle modernization program is fairly well structured, with a clear roadmap to update legacy platforms and GVA forming the baseline and easing integration. In the medium-to-long term, Morpheus will obviously be the clear determinant, but until that direction is settled there are three main projects in play.

As of now, the Bowman rollout has ensured that all battlefield vehicles have a degree of connectivity with specialized BCIP outfits, but the introduction of the new Scout vehicle from 2017 will set a new benchmark in integration. Its new suite of sensors are all being developed by Thales within the GVA framework to seamlessly transfer the imagery and video around the vehicle, and stream it to other battlefield assets.

Similar – if cut down – capabilities are envisaged for the legacy Warrior fleet. However, that project appears permanently poorly timed and facing postponement. Lockheed Martin UK is the lead integrator for the project (and also the turret provider for the new Scout) and it successfully passed a number of key testing milestones in 2014, but is now waiting for a Critical Design Review in May 2015. At that point, the MoD may finally put in a production order to meet delivery deadlines currently expected for 2018, but as the CDR clashes with the UK's general election, it may once again be pushed back in the calendar.

The other major legacy upgrade project is a life extension for the Challenger 2 main battle tank that is likely to see the vehicles stripped right back to the metal and refitted with an improved GVA-compliant digitization suite, but the upgrade has already been postponed and descoped once (including ruling out an upgunning) and a decision on exactly what a resurrected project would encompass has been knocked back until after the election.

The army's protected patrol vehicle fleet – comprising all of the surviving mine-resistant, ambush-protected (MRAP) vehicle types – are undergoing a reset process to make them better suited (and legally compliant) to life in Europe, but as far as their connectivity goes, the army's plans are currently based on retaining their Bowman systems.

Another layer of UK battlefield connectivity infrastructure is provided by Cormorant, which provides joint force theatre communications and was declared operational in December 2004, but did not achieve full capability until 2007. Just two years later, it was found not to be able to provide the required capacity required by UK forces in Afghanistan and a replacement system was urgently acquired off-the-shelf in the shape of the Israeli Radwin 2000. This proved successful, but was in turn replaced in theatre by Falcon.

In fact, although Cormorant remains in service, Falcon is now the UK's main battlefield communications network. It was ordered to replace a raft of systems including the army's Ptarmigan and RAF Transportable Telecommunications System under a 2006 contract to BAE Systems. It was originally to be in service by 2010, but didn't complete field testing until mid-2012. However, by early 2014 deliveries had been completed and systems were operational with the army and air force.

It appeared ambitious at inception, with a decision to adopt an all-IP solution, but that has been vindicated as most other systems have taken that route too. It was designed for IPv4, but can switch to IPv6.

As it is so newly into service, Falcon is unlikely to be replaced any time soon, although upgrades and additional capabilities are a certainty. A preplanned enhancement was to get Falcon aboard navy vessels, but it is unclear whether this is still planned or if there is an agreed timeframe to roll it out.

2.3.2 France

France has a number of programs underway to modernize its digital connectivity. For the army, the key umbrella for several initiatives is the Synergie du COntact Renforcé par la Polyvalence et I'InfovalorisatiON (SCORPION) project that began in February 2010. Unusually amongst its UK and German peers, which have tended to conduct separate equipment acquisition projects and then work to combine the resulting systems, SCORPION has adopted a holistic approach aiming to enhance the country's land forces with new vehicles, weapon systems, networking equipment in an integrated, cohesive whole.

This means that the top line cost figures appear very high (the DGA is expected to signs cheques totalling 5 billion euros), but that's because it combines a host of new acquisitions. The biggest spend covers the purchase of around 2,500 new VBMR and EBRC armoured vehicles, and the upgrade of the Leclerc battle tank, all tied together by a new suite of integrated communications capability known as Système d'Information et de Combat SCORPION (SICS), which will also link the armour to unmanned systems and helicopters for closer coordination. The latter is in part the result of hard air/land integration lessons learned while fighting in Afghanistan where ground forces initially struggled to call on available close air support and close combat air assets.

The SCORPION architecture aims to enable Groupements Tactiques Interarmes (GTIA) – battlegroups of 500 to 1,500 personnel drawn from infantry, artillery, armour and engineering formations – to be deployed in cohesive, networked groups. The schedule is quite punishingly tight and will likely have to be revised as the first 18 GTIAs are supposed to be digitized between 2014 and 2020 (and a second group between 2018 and 2023). Planned budget reductions would have pushed these timelines back, but in the aftermath of the Charlie Hebdo attacks and apparent rise in Islamist threat, the government is reconsidering its defence spending.

Functionally, SICS will replace the elderly Système d'Information pour le Commandement des Forces (SICF) – which is made up of a range of different systems – with a single architecture.

SICS will embody a whole sweep of upgrades to be applied to the remaining battlefield vehicles not being replaced or recapitalised by the whole SCORPION project.

Development of the first version of SICS was awarded to Bull Systems – to the surprise of many, including EADS and Thales – under a 40 million euro contract awarded by the DGA in June 2013, ahead of deliveries expected to begin from 2016.

There are few exact details of the SICS equipment and structure, but Bull states that it will be highly autonomous and secure, providing connectivity across all layers of command. Additionally, Bull explained that its winning bid

> borrows methodologies and technologies from the civilian sphere, ruggedizing them for military requirements" and "the use of open technologies should cut the total cost ownership of tactical oper-

> ational information systems and offer greater scope to evolve the system to keep pace with future needs.[11]

The DGA has embarked on a sweeping communications modernisation project, known as Communications Numériques TACtiques et de Théâtre (CONTACT), which is looking to introduce common new software-defined radios to replace legacy systems such as Thales' PR4G, but still backwards compatible with legacy systems to ease integration.

The first phase began in June 2012 with a 1.06 billion euro contract awarded to Thales for 2,400 new radios (around 2,000 of which are to be vehicular, the remainder handheld) to equip two amphibious brigades by 2018.

At the same time, Thales began deliveries of a new battalion-level combined-arms headquarters communications node in 2014. The Réseau Intégré des Transmissions Automatiques (RITA) N4 node is an IP-based system affording access to Syracuse satellite communications, Link 16, VHF and HF radio networks as part of the army's Astride theatre communications system.

Thales is to deliver a total of 60 nodes, 20 handed over in mid-2014, another 20 should follow in 2015 and then another the following year, with an upgrade of 150 legacy RITA NG nodes up to the Astride standard. The French Air Force may acquire its own versions to equip deployable / forward airbases with Link 16 and other connectivity.

These deliveries followed a study – known as ETO AGORA – awarded to Thales by the DGA in January 2014 to define the overall system architecture for future joint French network-centric operations in the 2020 to 2025 timeframe. This would in turn define how all of the services provided by Astride and other networks could be delivered in a coherent manner together with COMSAT NG, COMCEPT, SATCOM and the RIFAN naval fleet network, along with new networking technologies such as 4G LTE. The results of that study have not yet been made public.

France is also poised to introduce an evolved version of its Fantassin à Équipement et Liaisons Intégrés (FELIN) integrated infantry equipment and communications suite.

[11] "French Defense Procurement Agency (Direction Générale de l'Armement, DGA) Turns to Bull to Develop Initial Version of Its Scorpion Combat Information System", in *Reuters*, 17 June 2013, http://www.reuters.com/article/bull-idUSnBw165020a+100+BSW20130617.

In many ways, FELIN is the most advanced of all the soldier digitization systems in development, with a wealth of experience fed back into development from Afghanistan, Chad, Mali and other deployments. Experience of the SitComDé (Système d'Information Terminal-Combattant Débarqué) combat information/battle management system from those theatres points to it working well.

However, one of its weaknesses – to be addressed with from 2016 – is that, in a similar manner to the vaguely disconnected architecture of the German IdZ, France currently uses three separate C2 systems from three manufacturers covering command levels from the dismount up to formation commands. Unlike the German situation, the French Army has at least managed to integrate the systems successfully, but when FELIN V2 comes in, the army will transition to a single structure.

Other modifications within FELIN V1 are related more to soldier ergonomics, with new cabling, modern displays and so forth, but a V2 competition will look to rationalize the capabilities and hardware elements of the system.

Sagem has looked to export FELIN as an off-the-shelf system, and France has discussed sharing development of future iterations with the UK but it is extremely unlikely that France would itself buy a prêt-a-porter solution. It is also debatable how much it could realistically share development of an integrated soldier system with the UK or Germany, as each force is wedded to so much of its own bespoke equipment tailored to slightly different operating concepts.

It emerged in early 2015 that French Army Light Aviation elements had added an important new layer of connectivity as an upgrade to its specialist Système d'Information Terminal de l'ALAT (SIT-ALAT), linking it together with the Système d'Information Régimentaire (SIR) and new Helicopter Mission Trainer (HMT) simulation. This enabled 18 elderly Gazelle and Puma helicopter crews to fly a coordinated training exercise – known as Aozou – together with 12 virtual helicopters flown by crews in the HMT simulator. This was a key test for Miccavionics' C2 software that the company has developed for Bull as a vital element of SIC-S and will integrate with SIT-ALAT. The first operational version of SIC-S is set for fielding in 2016. The success of Aozou bodes well for the roll out of SIC-S as it demonstrated the ease of integration of disparate platforms.

2.3.3 Germany

German military communications specialists have faced the same issues as the British and French, particularly regarding coalition and joint interconnectivity as highlighted by the hothouse of operations in Afghanistan. However, Germany perhaps encountered a bigger issue on operations than the other two, as it discovered that its piecemeal and episodic digitisation was not as integrated as might be wished.

Germany's biggest ticket battlefield communications and digitisation push is intimately bound up in the fate of the army's Infanterist der Zukunft Erweitertes System (IdZ-ES) integrated soldier system.

The Bundeswehr placed its first order for IdZ kits (being developed first by EADS – now Airbus – and then later by Rheinmetall Detec) in 2004, with an eye to deploying the systems into Afghanistan to secure some early operational feedback. After several evolutions and studies, the first batch of 30 production-standard IdZ-ES soldier ensembles was handed over to the German Army in December 2012. Multiple lots followed, sized to outfit the various Einsatzverband (battlegroups) in Afghanistan, but then stopped in March 2014 when the last of 900 ordered ensembles was delivered.

Additional funding has now been allocated into the Bundeswehr's long term costings and Rheinmetall is expecting orders in early 2015.

Rheinmetall has disclosed that some elements have been overtaken by technology developments in the wider world. For example, the display elements of the German soldier systems are powered by now-outdated Windows-based portable computing because they were developed before the extraordinary rise of the smartphone. A version of IdZ offered to Canada was based on the Android operating system and this is understood to now form the basis for a rebaselined IdZ.

Rheinmetall is also working to develop a data interface to bridge the earlier generation IdZ-Basissystem (BS) to the latest generation IdZ-ES to ensure as much re-use and continuity as possible.

By all accounts, the systems proved effective and popular with soldiers deployed to Afghanistan, but its utility was hampered by a lack of direct connectivity above the squad level.

The individual ensemble's Thales SOLAR 400EG-E radio provided intra-team and squad secure voice and data, while a Thales SOLAR 400V rebroadcast version mounted into the squad's Boxer armoured personnel carrier offered extended range to connect with other elements. However, the system had no data connectivity to the Airbus-developed battalion-level Führungsinformationssystem Heer (FüInfoSys-Heer/FIS-H), forcing squad leaders to revert to insecure, fixed-frequency Thales SEM 52SL VHF radios to connect with platoon or company echelons using voice only.

Meanwhile, the Bundeswehr had managed to enable a degree of interoperability between IdZ-BS and FIS-H – both developed by Airbus – using proprietary symbology developed by Airbus, but that differed from the MIP-DEM standard adopted for the later IdZ-ES. Although this illustrates the dangers inherent in even selecting agreed standards, it is also a salutary lesson that shouldn't be encountered again in the near future as open standards are becoming the norm.

Rheinmetall and Airbus were jointly contracted to find a data interface workaround in 2012 and the army trialled the resulting solution – adding a modified ATM KommServer translator connected to a Thales SEM 93 16 kbit/second secure radio deployed with the new Puma armoured vehicle. Although this appears to work, it is not a permanent solution because the older VHF SEM radios' data throughputs lag way behind those achieved by the SOLAR 400 UHF systems used at the tactical edge.

In November 2014, Thales delivered the last of a batch of SEM 600A V/UHF radios with broadband capabilities, which was just in time as the new Puma crews and battalion commanders are scheduled to begin full training in mid-2015.

The Bundeswehr plans to eventually base all of its future vehicle communication solutions on a developmental software communications architecture (SCA)-compliant Streitkräftegemeinsame Verbundfähige Funkgeräteausstattung (SVFFuA) joint software-defined radio range of systems.

Harris' AN/PRC-117G radio – as used by German special forces in Afghanistan – has been fitted aboard its new Leopard 2A7 tanks handed over in December 2014 and is also set for the Puma. The PRC-117G is SCA-compliant and could fit the SVFFuA bill (it could accommodate SCA versions of the German SEM VHF waveforms), but has so far only explicitly been selected for SATCOMs connectivity.

The army also plans to rapidly field a new longer-range, handheld data radio integrated with the IdZ-ES as part of the squad leader's ensemble to provide connectivity with higher echelons and get around the legacy voice-only issue. The Bundeswehr plan expected all three services to select a suitable option for this requirement, but the army is now expected to make a selection that the others may – or may not – also adopt because the lack of connectivity needs to be urgently addressed.

Other important communications upgrades are being applied to the Bundeswehr's Thales-primed BIGSTAF (Breitbandiges, Integriertes GefechtsSTAnd Fernmeldenetz) wide-band, integrated command post communications network. In 2013, Steep GmbH and Blackned GmbH were contracted to replace the legacy fibre-optically wired elements of FIS-H with the new voice over IP-based Mobile Unified Platform communications.

In some ways, Germany is in a luxurious position as its vehicle fleets are relatively new or in the process of being replaced. As such, these modern vehicles have been designed with modern C3 fits in mind and are set for no more than routine upgrades as systems are introduced or upgraded in the near future.

However, as described with the radio issues for Afghanistan, the vehicles deployed there had to be upgraded for theatre and the army is now resetting and working towards a common fleet.

German army connectivity is nevertheless facing some issues as the new types filtering into service are absorbing funds and the government is reluctant to spend more on the elderly vehicles they are replacing, so some mismatched capabilities are inevitable. After some delays, the tracked IFV fleet is now re-baselining on the Pumas as the old Marders are phased out and the new Boxers are steadily replacing the Fuchs fleet. At a lower level, the Dingos and Eagle Vs are essentially new vehicles with modern electronics and interfaces.

An interesting throwback that rather questions Germany's commitment to full-scale adoption of modern communications systems is the determination to continue fielding a wired telephone into the rear of its Leopard 2 MBTs to ensure connectivity with dismounts.

2.4 Satellite Communications (SATCOM)

2.4.1 United Kingdom

The UK's military satellite telecoms service is provided by the Skynet constellation and associated ground infrastructure. The service has been cyclically upgraded since Skynet 4B was launched in 1988 and is currently up to Skynet 5. The fourth and final satellite for this latest iteration – Skynet 5D – was launched in December 2012 (it was on station and operational by April 2013) and the constellation is relatively stable for now.

However, the satellite build and launch market is a cycle of troughs leading to launch peaks, followed by funding drop offs as the capabilities fall back on support contracts. Accordingly, at some point in the next five years, the UK will need to start the replacement process for Skynets 5A-C.

The whole Skynet project was the result of an innovative private finance initiative with Paradigm Services (setup by EADS – now Airbus) worth around 2.5 billion pounds and the largest that the UK MoD had ever had to that point. Under the deal, Paradigm provided the UK with an agreed bandwidth of assured access to secure SATCOMs, but is able to use the rest of the network's capacity for other means.

Paradigm is currently under contract to continue provision until 2022 and all indications are that the deal is working to the satisfaction of the MoD.

The Anglo-French defence cooperation accord signed in 2012 set out a specific provision for satellite communications: "France and UK will look to confirm their intent to adopt a cooperative approach to meet their need for future COMSAT services, considering they will form a core asset in any Beyond Line of Sight capabilities in the future."[12] Three years on, that has yet to deliver any concrete developments, at least as far as the satellite infrastructure is concerned. France's decision in January 2015 to proceed with its own satellite launches would seem to point up that any cooperative deal would be more likely to involve the sharing of bandwidth, rather than true multinational development and cooperation on a par with the Franco-Italian deals.

[12] UK Prime Minister's Office, *UK-France declaration on security and defence*, 17 February 2012, https://www.gov.uk/government/news/uk-france-declaration-on-security-and-defence.

Since the UK's Skynet satellites are already the subject of an unusual ownership deal with a commercial entity, it is not beyond the realm of possibility that the UK will countenance further capacity sharing with its European partners in future. Indeed, Skynet capacity has already been used by Australia, Canada, France, Germany, the Netherlands, Portugal and the US.

Whether this would extend to jointly developing satellites for a follow-on capability remains to be seen, but the UK is likely to want to retain it as a sovereign capability and joint development projects to date have not borne fruit.

In the meantime, the UK MoD once again demonstrated a pragmatic approach to securing satellite bandwidth and airtime in early March 2015, when it signed a 12-month contract with Airbus Defence and Space to support friendly force tracking. The deal will use Iridium Short Burst Data and Iridium Rudics Data Minutes to support the Ground Asset Tracking System (GrATS) and Helicopter Asset Tracking System (HeATS) with near real-time reporting of GPS data from all suitably outfitted elements.

2.4.2 France

France seems to have lost faith in a multinational cooperative program under EDA/ESA frameworks and is preparing to go it alone once more, as it needs to make a selection to ensure it maintains its capabilities and is expected to order two new military communications satellites from Airbus Defence and Space and Thales Alenia Space in early 2015.

These satellites are part of COMSAT NG (Next Generation) and – along with new ground infrastructure – could cost a total of 800 million euros, aiming to get the first new satellite into service by 2021 to replace a pair of Syracuse 3 satellites.

Unlike Germany and the UK, France has not been able to agree a PFI or industry-managed project, so the program will have to be entirely funded from the defence budget. There is some debate about whether this will work out cheaper than the service costs that the UK pays to Airbus for Skynet, but the details of French projections are not public to make a straight comparison.

That's not to say that it hasn't tried to outsource the capability: in 2010 the DGA planned to sell the Syracuse 3 satellites back to industry, then lease back guaranteed availability for an annual fee in a similar situation to the UK's Skynet deal. The satellites at that time had a latent over capacity of approximately 10%, which the DGA assumed the new satellite owners would just lease on to somebody else, but in March 2012 the whole project was scrapped.

For one thing the deal was not sufficiently attractive to industry and for another, the government's vacillating over the concept had eaten into the satellites planned 15-year lifespan, reducing their trade-in value for the treasury's coffers.

France has, however, been able to negotiate a shared equity/shared payload deal with Italy, which resulted in the ATHENA-FIDUS satellite being launched piggy backing French and Italian broadband payloads onto the same asset in early 2014 and a subsequent SICRAL 2 satellite (also with Franco-Italian SATCOMs payloads) is set for launch in the middle of 2015.

There are obvious cost-sharing benefits of this paired approach at the national level, but from a multinational pooled capacity perspective it is a decidedly negative situation as the two payloads are – by definition – in the same orbit, reducing the potential coverage benefits that could be gained were they not hosted together.

Nevertheless, France boasts the largest range of military satellites of the three countries, with several key projects in place, notwithstanding the age and approaching obsolescence of them.

The oldest of the current generation of satellites are the Syracuse 3A (launched in October 2005) and 3B (August 2006), which provide global voice and secure datalinks and are used for command and control, intelligence sharing and logistics.

The earlier Syracuse 1 and 2 were piggybacked onto French civilian Telecom satellites, but the "3" generation were dedicated military-specific platforms and are hardened against attack, nuclear electromagnetic and countermeasure interference. Their exact throughput is classified, but it is understood to be in the order of several hundred megabits/second and easily sufficient to support video conferencing and a degree of cloud computing.

Of course, the downside to all that capability is cost: the current Syracuse was valued in the order of 2.3 billion euros to prime contractor Alcatel Space (now Thales Alenia Space) and Thales Communications (responsible for the ground segment). The DGA has access to roughly 600 fixed and mobile networked stations, along with a number of SATCOM on the move terminals acquired originally for service in Afghanistan, but which have now been deployed on operations in Africa.

Access to the satellites is very much a joint affair, with dismounts, vehicles, aircraft, submarines and warships all getting access, and the satellites themselves being rated compliant with NATO's STANAG 4606 security standards. The communications bearers are SHF/X-band and EHF, the latter of which is not compatible with US systems as the EHF signal processing is not conducted on board the satellite.

France now has a partial replacement plan underway with the SICRAL 2 and ATHENA-FIDUS projects in play with Italy.

For its part, the EHF/Ka-band ATHENA-FIDUS was launched into a geostationary orbit in February 2014. It is a less military-specific system than Syracuse, using high-performance civil communications standards (DVB-RCS and DVB-S2), and should stay operational for more than 15 years. It does not boast advanced anti-jamming capabilities, but it does have high transmission datarates above 3 gigabit/second.

SICRAL 2 is still in build and aims to combine elements of Italy's SICRAL 1 with France's Syracuse 3. It is set for launch in the first quarter of 2015 and will be geostationary, with a UHF/SHF payload and a life expectancy out to 2029 that should ensure a bridging capability is maintained for France spanning the de-orbit or retirement of Syracuse 3 before the end of this decade and the introduction of the COMSAT NG.

In the same month that the ATHENA-FIDUS satellite lifted off, Thales Alenia Space announced a contract from the DGA to provide operational support for all three main SATCOMs systems – Syracuse 3, SICRAL 2 and ATHENA-FIDUS – lasting out to 2031, so it appears that France is a closed shop for some time to come on that score.

The final segment of French SATCOMs is swept up in the COMCEPT (COMplément de Capacités en Elongation, Projection et Théâtre) program. Thales ran an architectural study for the DGA in 2010 and the resulting package was contracted to Airbus Defence and Space Services, partnered with Actia Sodielec in February 2013.

In essence, it is designed to deliver a Ka-band ground segment for the French Army, Air Force and Navy providing them with fast (10 megabit/second), secure broadband communications. This will then be usable for full-IP video, telephony and data exchange for static and deployable, mobile systems: elements will be integrated into manned and unmanned aircraft, ships and vehicles.

Airbus completed its first end-to-end COMCEPT to ATHENA-FIDUS link in June 2014 and under the current deal, the project support is set to last 17 years.

2.4.3 Germany

Germany's own military SATCOMs provision is delivered by the two-stage COMSATBw satellites developed by Astrium and are still relatively early in their service lives.

COMSATBw-1 was lofted into orbit in October 2009, followed on 21 May 2010 by COMSATBw-2, both with a design life expectation of 15 years. This means that even accounting for the years-long gestation period required to build and launch satellites, there is no immediate pressure for Germany to create a new generation and there is currently no known successor or follow-on plan.

Both COMSATBw satellites are in geostationary orbit, one over the Indian Ocean and the other over Africa, giving an indication of Germany's areas of interest. They deliver secure voice and data using four SHF and five UHF transponders, with ground terminals providing uplinks in the order of 6 megabit/second.

The satellites themselves were built by Thales Alenia Space and delivered to EADS Astrium (now Airbus). Germany has outsourced running the satellites to a large degree and they are managed by Astrium's Milsat Services subsidiary, with the ground segments handled by LSE Space, leaving the Bundeswehr to approach SATCOMs as a customer, without the overhead of having to manage the network (but also without the ability to take over directly should that become necessary).

Beyond COMSATBw, Germany also has lease agreements in place to buy commercial SATCOMs bandwidth from the privately owned Intelsat constellation.

In addition, when Germany has needed extra capacity beyond that offered by the Bundeswehr's national capability, it has acquired bandwidth from partners such as the UK's Skynet constellation and US assets on loan. However, Germany has encountered challenges in sharing out its own capacity with coalition partners by German federal laws, which prohibit bandwidth being given away without compensation. This proved particularly challenging for German forces deployed with ISAF, which tended to involve a range of ad hoc and flexible asset sharing policies, and Germany may need to revisit those legal constraints in future.

Additionally, the growth of data hungry operations and Germany's increasing propensity for out-of-area operations (including naval deployments to the Horn of Africa, army and air force operations in Afghanistan, as well as peacekeeping tours from Rwanda to Georgia) may force the Bundeswehr to seek out additional capacity, but there are no concrete plans at the moment to add a COMSATBw-3.

2.4.4 EDA framework

France, Germany and the UK are all members of a SATCOM user group set up by the European Defence Agency (EDA) – together with Italy and Spain – in 2014 to explore the potential for shared provision of non-hardened (but still secure) government SATCOMs.

An initial study looking to identify operational needs was completed in 2014 and transitioned to a gap analysis study in 2015 that has aspirations to help channel some research and development money and establish an EU-wide roadmap.

The EDA has estimated that sharing the capacity of these five countries could save in the order of 2.5 billion euros, but the agency does not have a great track record of delivering tangible results from this kind of study. In fact it has been seeking efficiencies from pooling the capacity since the mid-2000s with very little success. Even though the ESA has established a very solid reputation in the commercial space world, this latest initiative does not appear to be gaining any traction in the near future.

The main stumbling block is that the lifespans of the legacy national satellite constellations is out of sync: Germany has at least ten years left for COMSATBw and the UK is still a few years away from needing to think about replacing Skynet 5, but France is rapidly running out of time and should, ideally, have started moves to recapitalise last year. It has had more luck working with Italy, which has similar timeframe pressures.

The EDA, however, has had a degree of success – albeit at a low level – with the European Satellite Communication Procurement Cell (ESCPC) set up by the agency and Airbus' Astrium subsidiary in September 2012. In essence, the cell pools requirements across a group of users and uses that greater buying power to secure commercial satellite access at cheaper rates.

In early February 2014, it announced that it had "facilitated" orders of more than 1 million euros.

> Three additional contributing Member States (Belgium, Finland and Luxembourg) have joined the five ESCPC founding nations (France, Italy, Poland, Romania and the United Kingdom) while others declared their interest in the pay-per-use scheme.[13]

It went on to claim that it reduced costs for users of the scheme by 20% and later that year France capitalized on the partnership by buying satellite capacity to support its operations in Mali at short notice.

There are no more recent usage figures available and although it would be churlish to dismiss 20% savings, in the grand scheme of national satellite costs the apparent usage of the ESCPC specifically is not reaping huge sums of money.

2.5 Naval connectivity

From a naval perspective, all three countries are actively involved in programs to digitally network their naval assets, but on nothing like the same scale as the US Navy.

For example, none of them have bought into the US Cooperative Engagement Capability (CEC). In essence, CEC is a data fusion system that

[13] European Defence Agency (EDA), *Progress for European Satellite Communication Procurement Cell (ESCPC)*, 5 February 2014, https://www.eda.europa.eu/info-hub/press-centre/latest-news/2014/02/05/progress-for-european-satellite-communication-procurement-cell-(escpc).

draws together and combines data from a wide range of radars and combat management systems (principally the Hawkeye airborne early warning aircraft's APY-9 radar and the SPY radars carried by Aegis-capable warships) affording warships and aircraft access to a shared air picture. This is heavily automated and provides details of single recognized tracks, enabling operators to easily apportion engagement tasks to the most appropriate asset.

The US Navy is so enamoured of the concept that it is now exploring an extension of the approach under a "Distributed Lethality" project that could see missile launch cells fitted to a much wider range of surface vessels – including support types and amphibious ships – in theory enabling them to engage surface and air targets cued by off board sensors.

This is far in advance of anything being attempted by France, Germany or the UK. The UK planned to adopt CEC and indeed the Royal Navy conducted a series of trials in the early part of the last decade, expecting to acquire installations for the Type 23 Duke-class frigates from 2008 and then Type 45 Daring-class destroyers from 2012 in a project valued at around 400 million pounds.

However, funding issues and the distraction of simultaneous operations in Iraq and Afghanistan led to the project being put on hold in 2005. In its place, the UK Ministry of Defence embarked on an ill-fated joint-service network engagement capability program known as the Operational Capability Demonstrator.

In the meantime, the UK continued funding a minor stake in CEC, with two batches of money allocated in March and April 2010 under the US Foreign Military Sales program in support of UK involvement. That never led to a CEC procurement and in early 2012, the acquisition program was formally dropped, with the MoD citing budget constraints.

Germany also indicated interest in CEC in the mid-2000s, but nothing formal ever came of that and Germany is not known to have an indigenous capability.

In France, the Direction Générale de l'Armement (DGA) and French Navy held a joint program with DCNS and Thales known as the Tenue de Situation Multi Plates-Formes (TSMPF) or Multi-Platform Tracking Capability, as a demonstration platform for a Capacité d'Engagement Multi Plates-Formes (CEMP) that was roughly analogous to CEC.

Details of this project were briefed at the MAST conference in Cadiz in 2008 and work was known to be underway the following year, but it subsequently sank from view.

At root, it appears to have just been a simulation project exploring concept architectures for how a cooperative engagement network could function, resulting in the suggestion that such a network would be possible by acquiring some new system elements and mating them with legacy communications and battle management systems in a hybrid form.

The only country known to have joined in with CEC is Australia, which is acquiring the capability for its new Hobart-class Air Warfare Destroyers. Japan may also end up joining in, in due course, but at a European level, the majority of naval networked connectivity is limited to more conventional communications and datalinks, particularly through NATO Link 16 and 22, the latter being driven in no small part by Germany.

2.6 Air connectivity

France is looking to extend the time-sensitive targeting loop tried out aboard Charles de Gaulle during Operation Harmattan strikes against Libya, applying the concept to the French Air Force.

At its heart, the concept is a pure NEC concept, using a Thales-developed TDH 6000 secure digital datalink to downlink high resolution imagery (at rates of >100 megabit/second) from the Thales Reco-NG reconnaissance pod over ranges of up to 350 km.

The French Navy’s novelty was forward-basing a targeting cell complete with SAIM-NG (Système d’Aide à l’Interprétation Multi-capteurs) multisensor image interpretation and dissemination systems to enable rapid targeting turnarounds and the air force is now looking to adopt a similar approach. For its operations against rebels in Mali, the air force deployed its targeting cell at its host air base, but in 2015 it plans to trial installing SAIM-NG workstations aboard a C-135 tanker to accompany the strike aircraft, radically shortening the sensor to shooter loop.

Onward dissemination of the data analysis will be via NATO-standardized voice or data links, which opens up the capability to coalition forces, but still relies on French aircraft with Reco-NG pods are not widely used.

Curiously, although the UK is watching developments closely, it is not believed to have any plans for accelerating its own targeting capabilities in a similar manner and is not a fan of the US concept of forward deploying FAC-A airborne forward air controllers.

2.7 Conclusions

France, Germany and the UK have a lot in common and are all facing similar challenges with regard to digitizing and connecting their forces, but in the main they are still developing individual paths toward the goal of NEC. Their positions within NATO will ensure that the various national systems will have some degree of interoperability at touch points between them. Initiatives such as the NATO Future Mission Network will see to that by standardizing basic interfaces. However, that will just enable the various nationally networked battle management and communications systems to interface at a relatively high – headquarters – level, it will not enable a FELIN-equipped soldier to seamlessly work with their IdZ-laden comrade in anything like the short term.

Interconnectivity is important, but it does not produce the same detailed granular capability as when forces are all working seamlessly within the same network.

France is probably the most committed of the three nations to establishing a true network enabled force, with FELIN already well established and the country's coherent SCORPION plans to recapitalize its land forces.

The UK isn't far behind, and its LE TacCIS plans should deliver a similarly cohesive capability, now that MoD planners have the time and brain space to be able to map out a sensible path, rather than being constantly ambushed by urgent operational requirements being fielded to help out troops in the field. However, the project's success remains to be seen as the plans are rolled out.

Germany too has sensible plans in place to pull together its disparate systems and apply the lessons learnt on operations, but the Bundeswehr's budgetary pressures and lack of consistency may continue to hamper its ambitions. To be fair, that could be said of all three countries.

Although the number and seriousness of cyber attacks continue to grow at an alarming rate, so far they have mostly been conducted against civilian infrastructure or low-level denial of service attacks against military websites or social media targets, with little impact at a tactical or even operational edge. As a result, French, German and British military forces have yet to feel a real impetus – as opposed to a financial or organizational / strategic imperative – at a national level, let alone a need to join together operationally at a multinational level to combat the threat beyond sharing information. Counter intuitively, perhaps that is one of the strengths of an uncoordinated multinational approach to networking, communications, cyber and SATCOM: if the users and owners of the various national networks and capabilities struggle to get their own systems to work together, then maybe that provides an inherent defence against a concerted cyber attack.

3.
Italy and the Forza NEC Program

Tommaso De Zan

This chapter provides an overview of Forza NEC, the procurement program led by the Italian Army (IA) and started in 2007, which aims to develop a netcentric architecture with the goal to provide "information superiority" through the digitization of the armed forces. By adopting a very focused approach, Forza NEC intends to meet the operational needs of the Army acquiring specific assets and/or modernizing those already owned. In fact, the program has undertaken a significant stage of development and experimentation – the so-called "Concept Development & Experimentation" (CD&E) phase, which is the current phase of the program – to validate technological solutions in the light of operational requirements set by the Army, even through a continuous dialogue between the armed forces and the industry. Compared to what was previously envisaged, the acquisition of digital assets and/or the digitization of legacy platforms and systems will not occur all at once. Instead, the armed forces will acquire, and this is already happening through separate programs called "spin-offs," for those technological solutions deemed "ready" and suitable to meet the requirements of the Army. The program is unfolding in this manner not only because of the technological challenges posed by the application of ICT tools and principles to the military world, but also because of the Ministry of Defence budgetary constraints. At the same time, the aim is to ensure that the results of the CD&E will positively influence the overall modernization of the armed forces, linking Forza NEC with existing or future procurement programs.

The chapter is organized in five sections. The first describes the role of the Army in pursuing the objectives of the Italian defence policy, its main operational experiences since the end of the Cold War and possible future deployment scenarios. The purpose of this first section is to define the operational requirements that prompted the military to consider a Netcentric modernization. The second section explains what the NEC capability entails and its importance in the military domain. The section then analyses the advantages the Army may expect to gain from the acquisition of NEC capabilities and illustrates the transformation that the armed forces will undergo during the process of digitization. The third section outlines the industrial aspects of the program: the financial framework, the industrial organisation and its governance, the principles of management the program is relying on, and, finally, the various phases and timing of Forza NEC. The fourth section assesses the challenges and the opportunities deriving from the program, considering both its current and future perspectives. The fifth section concludes the chapter, providing some comments on the role of technology in the military and industrial domains.

3.1 The Italian defence policy and the role of the Army

3.1.1 The Italian defence policy

According to the "White Paper for International Security and Defence" (2015), the primary objective of Italian security and defence policy consists in the "is the protection of Italy's vital and strategic interests."[1] The document states that to reach this objective "the defence of the State and its sovereignty must be ensured, the construction of a stable framework of regional security must be pursued and efforts must be made to facili-

[1] Italian Ministry of Defence, *White Paper for International Security and Defence*, July 2015, p. 33, http://www.difesa.it/Primo_Piano/Documents/2015/07_Luglio/White%20book.pdf. The vital interests are "that set of elements which constitute the primary and mandatory needs of the Country, including self-preservation, territorial integrity and economic security." The strategic interests are instead "represented by the set of utilities, advantages, conveniences of great importance for a State. The failure to protect a strategic interest, while not jeopardizing the very existence of the State, undermines the social, economic, technological and cultural future, as expected to be if the interest were not compromised." Italian Ministry of Defence, *Linee guida del Libro bianco per la sicurezza internazionale e la difesa*, June 2014, p. 15, http://flpdifesa.org/wp-content/uploads/2014/07/Linee-Guida-per-il-Libro-Bianco.pdf.

tate the creation of a favourable international environment."[2] In this perspective, the Defence function and its operational tool represented by the military instrument, are an essential element of the national system of protection and guarantee of our freedom.

Since the Second World War, the regional security context surrounding Italy has led governments to invest in their relations with major international organizations of collective security and defence – namely the UN, the EU, NATO and OSCE – to ensure that Italian vital interests were protected more effectively than the country could guarantee on its own. Participation in these organisations was also essential to act in a security context base on a "shared consensus". The multilateral nature of such a "security architecture" has benefitted Italy as a recipient of international guarantees in the event of an armed attack or threat, but has required the country to actively devote resources in this "production of security" when international crises has occurred. Therefore, in addition to the "classic" aforementioned objectives, the Italian armed forces have conducted missions different from the mere protection of the territorial integrity of the State, especially since the end of the Cold War. As stated in the White Paper, the missions the Italian armed forces are asked to carry on in the pursuit of its defence policy objectives are:[3]

- To defend the State against any possible aggression in order to safeguard its territorial integrity, its national vital interests, the security of areas of national sovereignty and of fellow citizens abroad and ultimately the safety and integrity of the communication paths to access the country;
- To defend the Euro-Atlantic and Euro-Mediterranean regions by contributing to NATO's collective defence and by maintaining stability of the Mediterranean Sea area;
- To achieve peace and international security with the involvement in operations of crisis prevention and management in the spirit of the UN Charter;
- To safeguard free institutions and to carry out specific tasks in case of calamity or emergency.

[2] Italian Ministry of Defence, *White Paper for International Security and Defence*, cit., p. 33.

[3] Ibid., p. 42.

3.1.2 The role of the Army

The Army has a key role in achieving the objectives of Italian defence policy. The Army comprises of 103,000 soldiers and 9,800 civilians, in addition to 3,800 combat and 7,300 support vehicles, plus 226 helicopters. These are scattered in 3,900 facilities around the country. The figures will probably decrease due to the reform process that began in December 2012 with the Law 244/2012[4] and its implementing decree.[5] At the end of this process, the IA will consist of 9 brigades – instead of the current 11 – and will shrink to 90,000 soldiers and 9,000 civilians. Its infrastructures will be reduced by 40%.[6]

In the last two decades, the Army has deployed on average 9,000 units in international missions and 4,000 in domestic operations, with peaks of 19,000 soldiers simultaneously located in domestic and international theatres. In terms of quantity, and compared to the Air Force and the Navy, the AI is the most deployed armed force, providing approximately 75% of the total Italian soldiers in operational theatre.[7] In 2014, the Army has deployed its soldiers in 2 national operations and in 12 international missions, totalling 10,361 units in theatre.

What follows is a brief summary of the Army's involvement in the past two decades main operations. The summary highlights Army's effort

[4] Law No. 244/2012, "Delega al Governo per la revisione dello strumento militare nazionale e norme sulla medesima." The reform is based on four pillars: 1) a new limit on the overall number of Army, Navy and Air Force soldiers, which should not exceed 150,000 units; 2) the managerial staff of the three armed forces will be limited to 310 units; 3) a reduction of the armed forces infrastructures of at least 30%; 4) the reform will not burden on the annual state's budget, whereas all the savings the reform yields will be reinvested on the defence budget. See Alessandro Marrone, "I quattro pilastri della riforma della Difesa", in *AffarInternazionali*, 17 December 2012, http://www.affarinternazionali.it/articolo.asp?ID=2208.

[5] Law Decree No. 7-8 of 28 January 2014. According to the decree, which implements Law No. 244/2012, the Army will reduce its units by 13,400, the Air Force by 8,575, the Navy by 4,325 by 2024. However, according to some analyses, restructuring the military personnel by transfering them to other government agencies but only "with the prior consent of the concerned person" threatens to derail the reform process. For further details, see Alessandro Marrone, "La non riforma della Difesa", in *AffarInternazionali*, 24 February 2012, http://www.affarinternazionali.it/articolo.asp?ID=2544.

[6] Italian Army General Staff, *Linee di sviluppo evolutivo e innovativo dello strumento militare terrestre – PROSPECTA*, 2015, p. 6-7.

[7] Ibid., p. 16.

in the context of the Italian defence policy and explains how these operations contributed to determine the requirements of tools, assets and platforms that the Army will acquire in the years to come.[8] To this end, we will focus on operations in Kosovo, Iraq, Afghanistan and Lebanon. Notwithstanding the relevance and importance of other operations, (for example in Somalia and Bosnia), operations in the mentioned countries have significantly contributed in identifying existing capability deficiencies and thus to determine the new operational needs of the armed forces' land component.

Under the framework of UN Security Council resolution 1244, the IA is in Kosovo as part of the peacekeeping mission "Kosovo Force" (KFOR), following NATO's air campaign in Serbia and the subsequent agreement between the North Atlantic Alliance and the government of Slobodan Milosevic in June 1999. Italy deployed an initial contingent of 6,000 soldiers, second in size only to the one of the United States, showing the decisive commitment of the Army in an area of strategic interest for Italy.[9] Between 2004 and 2005, NATO authorities gathered all operations deployed in the Balkans in a single operational structure, creating the "Joint Enterprise" operation, which included the KFOR mission, relations with the European Union missions, and NATO HQs in Skopje, Tirana and Sarajevo.[10] Since May 2006, the international military force have undergone a reconfiguration, switching from four Multinational Brigades to five Multinational Task Forces, which later became known as Multinational Battle Groups on a regimental basis in 2010.[11] Starting on May 2011, the forces permanently stationed in Kosovo are two Multinational Battle Groups (one under Italian command), a Multinational Specialized Unit (MSU), which only includes the Italian Carabinieri, three multinational units called Joint Regional Detachment (JRD) – one of which is under Italian leadership – and, finally, a multinational regiment as a tactical reserve.[12] Since 2011, a total of 550 Italian soldiers belonging mainly to

[8] Interview, 10 February 2015.

[9] Fabrizio Coticchia, *Qualcosa è cambiato? L'evoluzione della politica di difesa italiana dall'Iraq alla Libia (1991-2011)*, Pisa, Pisa University Press, 2013, p. 158-171.

[10] Italian Ministry of Defence, *Kosovo - KFOR - Joint Enterprise*, http://www.difesa.it/EN/Operations/InternationalOperations/Kosovo_KFOR_JE/Pagine/default.aspx.

[11] Ibid.

[12] Ibid.

the Army have operated in Kosovo. Since September 2013, Italy has led the entire operation, which sees the participation of 31 countries, 23 of whom are NATO Member States and 8 partner countries.[13] Currently, the tasks assigned to Italian soldiers include the protection of security and freedom of movement, the supervision of the implementation of the Military Technical Agreement signed between Serbia and NATO, assistance in the development of local institutions and support to international organizations in the region.[14]

In March 2003, a US-led international coalition started the "Iraqi Freedom" operation in Iraq.[15] After the success of the coalition and UN resolution 1483 (22 May 2003), the second phase of operations began. The declared aim of the operation was the economic, social and political stability of Iraq.[16] Since August 2003, an Italian contingent of 3,000 soldiers – which increased up to 3,300 units in the spring of 2005 – has been involved in operation "Antica Babilonia" to restore security conditions, infrastructures and essential services in Iraq.

Italian soldiers were deployed to Nasiriyah, Baghdad and Basra, as well as in headquarters structures in Kuwait and Tampa (US). The Army had supervision of a sector in the province of Dhi Qar, under the Multinational Division South-East (MND-SE) led by the United Kingdom.[17] Italian soldiers were engaged in activities such as: training and equipping of Iraqi security forces, maintenance of the security conditions on the ground, reconstruction of infrastructures and essential services, NBC threat detection, besides humanitarian activities and projects to improve the quality of life, education and health care of the population.[18] The operation was considered by many "expensive, complex and dramatic," and

[13] Italian Ministry of Defence, *Kosovo - KFOR - Joint Enterprise, Contributo nazionale*, http://www.esercito.difesa.it/operazioni/operazioni_oltremare/Pagine/Kosovo-KFOR-Joint-Enterprise-contributo-nazionale.aspx.

[14] Ibid.

[15] Italy did not take part to this phase of the military operations.

[16] Italian Ministry of Defence, *Iraq - Antica Babilonia*, http://www.difesa.it/OperazioniMilitari/op_int_concluse/Iraq_AnticaBabilonia/Pagine/default.aspx.

[17] Italian Ministry of Defence, *Iraq - Antica Babilonia. Forze impegnate*, http://www.difesa.it/OperazioniMilitari/op_int_concluse/Iraq_AnticaBabilonia/Pagine/Forzeimpegnate.aspx.

[18] Italian Ministry of Defence, *Iraq - Antica Babilonia. Missione*, http://www.difesa.it/OperazioniMilitari/op_int_concluse/Iraq_AnticaBabilonia/Pagine/Missione.aspx.

suffered 33 deaths, the highest figure since the end of the Second World War if we exclude military operations in Afghanistan.[19] Italian soldiers operated in a highly confrontational theatre, which often constrained reconstruction or peace support activities. As a valuable example of that, one should remember the suicide attack against the "Mistral" base organized by Al-Qaeda in November 2003, which claimed the lives of 17 Italian soldiers and 2 civilians, plus 9 Iraqis. Italian soldiers were also involved in a series of high intensity battles, despite a general lack of resources and strict rules of engagement, in a context that requested combat rather than mere peacekeeping activities.[20] One can remember, for example, the three "battles of the bridges," in which Italian armed fought against the Mahdi' Army, made up of units of Muqtada al-Sadr. The Italian operation ended in December 2006, when the country's flag was lowered in Nasiriyah.

Italian forces have been operating in Afghanistan as part of "Operation Enduring Freedom" from March to September 2003 and in the framework of the International Security Assistance Force (ISAF) from August 2003 until December 2014. As for operation in Afghanistan, Enduring Freedom also falls in the context of the fight against international terrorism led by the United States following the dramatic attacks of 9/11. The goal of the mission was to create the conditions for a stable and secure Afghanistan through the elimination of the Taliban resistance movement and Al-Qaeda's threat, particularly in the Paktia province neighbouring Pakistan. The Italian mission "Nibbio," with a contingent of 1,000 soldiers, was tasked to "keep" the freed territory and to fight insurgent/terrorist groups. This activity also implied the destruction of their logistic bases and recruiting centres.[21] The mission can be considered one of the riskiest conducted by the armed force after World War II, given the theatre of operations' location along the porous border between Afghanistan and Pakistan, but also for the asymmetric threat that the troops had to face.[22] As for ISAF,

[19] Fabrizio Coticchia, *Qualcosa è cambiato?*, cit., p. 198-204.

[20] Ibid., p. 204-213.

[21] For a further dicussion on air-naval operations during the mission, see Vincenzo Camporini et al., *The Role of Italian Fighter Aircraft in Crisis Management Operations: Trends and Needs*, Rome, Nuova Cultura, March 2014 (IAI Research Papers No. 16), http://www.iai.it/en/node/2155.

[22] Italian Army General Staff, *Task Force Nibbio*, October 2013, http://www.difesa.it/

the mission began after UN Security Council resolution 1386 (2001) and against the backdrop of the Bonn Agreement (2001). The Italian operation started in August 2003, after NATO took responsibility for the mission.[23] The purpose of ISAF was to support the Afghan government in maintaining security conditions in the country, develop administrative institutions, extend government control over the territory, assist the humanitarian efforts and reconstruct the country.[24] In particular, Italian troops took care of training the Afghan army and police forces, the provision of humanitarian aid and the reconstruction of infrastructures.[25] The staff stationed in Kabul was primarily involved at the ISAF Command (ISAF HQ), ISAF Joint Command HQ (JC HQ ISAF), the Special Operations Forces Command (HQ ISAF SOF) and the NATO Training Mission-Afghanistan (NTM-A). The Italian armed forces of the Train Advise Assist Command-West (TAAC-W) operated in western Afghanistan, in the provinces of Herat, Badghis, Ghowr and Farah. Over the years, because of the deadlier Taliban guerrilla, the IA has been involved in a series of clashes against Taliban insurgents, especially in the Bala Murghab area.[26] The special forces of "Task Force 45" also operated in this area, mainly in the province of Helmand and on the border with Pakistan, to curb Taliban activities. They also conducted "Operation Sarissa" on the border with Iran.[27] Over the years, Italy has provided a significant number of troops and vehicles, responding adequately to the needs of the multinational force, especially at the time of the so-called "surge" implemented by the US administration in 2009. In support of the new US strategy, whose goals was to be achieved through a substantial increase of troops on the ground, Italy came to deploy up to

OperazioniMilitari/op_int_concluse/Afghanistan_Nibbio/Documents/92952_SchedaNIBBIO131003.pdf.

[23] Italian Army, *ISAF. Contributo nazionale*, http://www.esercito.difesa.it/operazioni/operazioni_oltremare/Pagine/ISAF-Contributo-Nazionale.aspx.

[24] Ibid.; NATO, *ISAF's mission in Afghanistan (2001-2014)*, last update 1 September 2015, http://www.nato.int/cps/en/natohq/topics_69366.htm.

[25] Italian Ministry of Defence, *Afghanistan - ISAF. Missione*, http://www.difesa.it/OperazioniMilitari/op_int_concluse/ISAF/Pagine/Missione.aspx.

[26] "Afghanistan: l'inferno di Bala Murghab", in *L'Espresso*, 21 July 2010, http://espresso.repubblica.it/internazionale/2010/07/21/news/l-inferno-di-bala-murghab-1.22554.

[27] "I soldati invisibili della Task Force 45", in *Il Sole 24 Ore*, 18 September, 2010, http://www.ilsole24ore.com/art/notizie/2010-09-18/soldati-invisibili-task-force-105713.shtml; Fabrizio Coticchia, *Qualcosa è cambiato?*, cit., p. 188-195.

4,000 people in 2011. In that year, more than a half of all soldiers and economic resources for overseas operations were dedicated to the Afghan operation.[28] Among the vehicles used, the Army employed CH-47, A-129 and NH-90 helicopters, VBM "Arrow" and LMV "Lynx" wheeled vehicles, C-130 and unmanned aircrafts. In the eleven years of mission, the Italian armed forces have suffered hundreds of attacks, killing more than fifty soldiers, the highest number of casualties in military operations since the end of the II World War.[29] ISAF was supplanted by mission "Resolute Support" in January 2015, to which he Army deploys 500 soldiers on an annual basis. The purpose of the mission is to train and assist Afghan security forces and institutions. Compared to ISAF, Resolute Support is not a combat mission and has a more limited number of units on the ground. Under current NATO plans, the first phase of the operation will end in July 2015, when most of the Italian contingent will head back. Approximately seventy units will remain in theatre until the end of 2015. The Army is the most consistent armed force within the mission, in particular with units from the "Garibaldi" sharpshooters Brigade, engaged in force protection and quick reaction force tasks, plus a component of the "Timavo" engineer corp, specialized in the management of explosive material and mines.[30]

The Army is currently involved in Lebanon in the framework of resolutions No. 425 (1978), 1701 (2006) and 1832 (2008), the latter two adopted following clashes and tensions between the Israeli forces and Hezbollah.[31] Italy, and in particular the Army, is part of the UNIFIL (UN Interim Force in Lebanon) multinational force under the aegis of the UN, which monitors the "Blue Line" armistice border between Lebanon and Israel since 1978. After the 2006 war, besides verifying the withdrawal of Israeli troops from Lebanese territories, the UNIFIL mission has also provided support to the Lebanese government to protect its borders and humanitarian assistance to the civilian population.[32] At the beginning of the "Leonte" national operation, Italy was among the countries that had most

[28] This data refers to all Italian armed forces deployed during the operation.

[29] Fabrizio Coticchia, *Qualcosa è cambiato?*, cit., p. 188.

[30] Italian Army, *RS: Contributo Nazionale*, http://www.esercito.difesa.it/operazioni/operazioni_oltremare/Pagine/RS-Contributo-Nazionale.aspx.

[31] Italian Ministry of Defence, *Operazioni Militari/Libano*, http://www.difesa.it/OperazioniMilitari/Pagine/scheda_ops_libano.aspx.

[32] Ibid.

contributed to the mission with 2,500 troops.[33] In addition to peacekeeping activities, the Army has mainly devoted its attention on civilian-military cooperation, land reclamation from explosive devices and specific programs in schools. As a demonstration of the Army's appreciated work, Italy took control of the entire UN operation for six of the last eight years of mission,[34] (the last time in October 2014) in an increasingly dangerous regional theatre considering tensions and instability generated by the civil conflict in Syria and the bloody advance of the Islamic State in Iraq and Syria.[35] The Italian contribution on April 2015 amounted to 1,100 troops.[36]

These operations have "tested" Italian soldiers in a variety of situations, requiring different skills and abilities because of the diversity of the tasks performed. The operating environment has proved to be:[37]

a) complex, joint and multi-dimensional;
b) characterized by asymmetric conflicts as opposed to traditional and/or hybrid ones;
c) expanded in space and areas of intervention;
d) characterized by multiple actors (both governmental and non);
e) interconnected in terms of platforms, sensors and actuators.

If one has to generalize in a nutshell what have been, and currently are, the main needs of the Army, last years' missions and operations have shown that, in the future, it would be desirable to: develop a C2 architecture able to collect and share information to effectively support the decision-making process in a timely manner;[38] expand the ability of real-time updates

[33] Fabrizio Coticchia, *Qualcosa è cambiato?*, cit., p. 220.

[34] Italian Ministry of Defence, *Operazioni Militari: Libano*, cit.

[35] "Lebanon under fire: Two years of spillover from the Syrian civil war", in *The Daily Star*, 16 January 2015, http://bit.ly/1JSUCaw; Carol Malouf e Ruth Sherlock, "ISIS Is Building Strength on Lebanon's Doorstep", in *BusinessInsider*, 20 January 2015, http://read.bi/15thyfi.

[36] Italian Army, *UNIFIL: Contributo Nazionale*, http://www.esercito.difesa.it/operazioni/operazioni_oltremare/Pagine/UNIFIL-Contributo-Nazionale.aspx.

[37] Interview, 10 February 2015.

[38] Command and Control is the "the exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission." Carl H. Builder, Steven C. Bankes, Richard Nordin, *Command Concepts. A Theory Derived from the Practice of Command and Control*, Santa Monica, RAND, 1999, p. xiii, http://www.rand.org/pubs/monograph_reports/MR775.html.

of the ground situation through sophisticated intelligence capabilities; and, ultimately, strengthen all new platforms with active and passive protection systems.[39]

3.1.3 Possible deployment scenarios

Although this possibility seems objectively remote, a first possible deployment scenario is the defence of the national territory in a classic conventional conflict between states, in which fighting forces are well defined and tend to avoid involving the civilian population.[40]

The second possible scenario is linked to the first, though perhaps more likely, and assumes that the IA would be involved in the defence of the euro-Atlantic region in case of attack on a NATO member state. Such an attack would activate article 5 of the Washington Treaty and the principle of collective defence.[41] For example, it is conceivable that the Army would take action following a deep political crisis within a member state of the Alliance, further exacerbated by internal ethnic minorities hostile to the political framework in place. Relying on these ethnic minorities, regional powers could fuel the conflict to increase their clout in their regional sphere of influence. An intervention could take the shape of an

[39] For the sake of completeness, in addition to those already mentioned, the operating theatres have also highlighted the following needs: improve close air support and ground artillery; promote better and greater integration of civil and military dimensions through dual-use capacities; increase the capacity ability of threat identification; improve emergency medical evacuation procedures; increase operational autonomy and logistics. Italian Army General Staff, *Linee di sviluppo evolutivo e innovativo dello strumento militare terrestre*, cit., p. 35.

[40] Ibid., p. 35.

[41] Article 5 of the Washington Treaty states: "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security."

armed forces mobilization as a deterrent, the securing of critical infrastructures (main roads, airports, etc.) or certain areas to ensure freedom of manoeuvring. In an extreme scenario, land forces might be called to engage enemy's troops in order to restore the territorial integrity of the occupied allied country.[42]

The third option is the possible deployment of the IA in crisis prevention, management and stabilization operations, especially in foreign countries beyond the perimeter of NATO.[43] In this scenario, a state might be destabilized by socio-political or ethno-religious tensions, escalating into a full civil war between a weak central government and one or more rebel groups. Following a resolution of the Security Council, Italian armed forces could initially intervene in a peace-enforcement mission[44] to prevent clashes between the warring parties and/or to protect the civilian population. After the end of the conflict, the mission might be refocused on peace-building activities[45] to create the conditions for a lasting peace. For this kind of mission, the Army might face an irregular or hybrid threat.[46] Besides purely military tasks, such as those of defence

[42] Italian Army General Staff, *Linee di sviluppo evolutivo e innovativo dello strumento militare terrestre*, cit., p. 35-37.

[43] Ibid., p. 44-45. Examples of these kind of missions are cited in the previous section.

[44] "Peace enforcement involves the application of a range of coercive measures, including the use of military force. It requires the explicit authorization of the Security Council. It is used to restore international peace and security in situations where the Security Council has decided to act in the face of a threat to the peace, breach of the peace or act of aggression. The Council may utilize, where appropriate, regional organizations and agencies for enforcement action under its authority and in accordance with the UN Charter." United Nations Peacekeeping, *Peace and Security*, http://www.un.org/en/peacekeeping/operations/peace.shtml.

[45] "Peacebuilding aims to reduce the risk of lapsing or relapsing into conflict by strengthening national capacities at all levels for conflict management, and to lay the foundation for sustainable peace and development. It is a complex, long-term process of creating the necessary conditions for sustainable peace. Peacebuilding measures address core issues that affect the functioning of society and the State, and seek to enhance the capacity of the State to effectively and legitimately carry out its core functions." Ibid.

[46] For irregular threat we mean the use of force typical of non-State actors such as terrorist groups or rebels who make extensive use of the strategy of terror. For hybrid threat we mean the threat caused by enemies whose nature is difficult to identify and which do not necessarily act on the basis of legal and ethical restrictions of State armed forces. They rely on practices of "attrition," through regular and irregular tactics executed in a concerted and/or combined manner. They effectively conduct propaganda/media operations.

and deterrence, there would also be other duties such as patrol missions and restoration of public order. The IA could be called upon to intervene in a "failed or fragile state," if the government of this country requests assistance in strengthening its defence capabilities, controlling its territory, reforming its security sector and consolidating its institutions.

The fourth and last scenario might bring about if the AI is called to support the Civil Protection or other institutional actors in the event of disasters or, more generally, in case of public needs. This is what happened, for instance, in L'Aquila after the earthquake of 2009 or more recently in Emilia-Romagna and Tuscany. The IA could be employed in the aftermath of a high magnitude earthquake, also followed by a tidal wave, if this has originated in a coastal zone. In a first phase, the armed force would be engaged in humanitarian activities in support of the affected population. Secondly, it would focus on the keep the area safe, in order to prevent looting and plundering.

In the future, the Army will continue to have a key role in supporting Italian defence policy, especially given the deterioration of the security regional context Italy belongs to. As recent years have shown, the unpredictability of the strategic framework has become an idiosyncrasy of the world the armed forces operate, together with the rapidity of its changes.

Although the possibility of a direct attack to Italy seems remote, at least from state actors, the fundamental role of the Army remains to defend the integrity of the territory. Even if unlikely, the possibility that Italy will be involved in a conventional struggle cannot be ruled out and this requires Italy to be ready to deal with threats that could become imminent in less than an eye blink.

Bearing in mind recent international events, the analysis of the second strategic option, namely the protection of the euro-Atlantic space, needs to be considered carefully. The 2014 crisis in Ukraine seems to have revived the spectre of a confrontation between the West and Russia, with many analysts now sceptical about the resilience of the post-Cold War European security system.[47] The consequences of the crisis have already

Italian Army General Staff, *Linee di sviluppo evolutivo e innovativo dello strumento militare terrestre*, cit., p. 50.

[47] Mikhail Gorbachev, "A New Cold War Order", in *Project Sindicate*, 5 January 2015, http://po.st/QpXoPk; Robert H. Legvold, "Managing the New Cold War", in *Foreign Af-*

emerged in recent statements and decisions adopted by Baltic and Scandinavian countries, the countries fearing the most the implications of the current crisis and the growing Russian activism along their borders.[48] NATO has also taken important decisions following the crisis. At the Wales summit in September 2014, member countries endorsed a Readiness Action Plan in order to maintain a high readiness in the event of a crisis. This readiness has been already tested by Russian activities in the proximity of Great Britain, the Baltic States, Sweden and other Northern European countries' sea and air spaces.[49] In such a context, a NATO intervention might be plausible if one of its member states is victim of the same tactics used by Russia to destabilize Ukraine, to the extent of a possible engagement with conventional enemy troops.[50]

It seems more likely, however, that in the future the Army will be deployed in situations similar to those envisaged by the third strategic option, that is in international missions whose operational environment will be similar to the ones where the armed force has operated in the past 25 years. Indeed, in areas located in the immediate proximity of Italy – North Africa and sub-Saharan Africa, Middle East, Eastern Europe, the Balkans and the Caucasus – non fully democratic countries or "frozen conflicts," features of new or recurring internal wars, are still present.[51] This option seems even more likely than the protection of the Atlantic area if one takes a look at Libya's current state of affairs. Following NATO's intervention in 2011, the North African country felt into complete chaos

fairs, Vol. 93, No. 4 (July/August 2014), p. 74-84, https://www.foreignaffairs.com/node/1113241; Stephen Walt, "The Bad Old Days Are Back", in *Foreign Policy*, 2 May 2014, http://foreignpolicy.com/2014/05/02/the-bad-old-days-are-back. More information on the Ukraine crisis can be found on the website of the Center for Strategic and International Studies (CSIS): The Ukraine Crisis Timeline, http://csis.org/ukraine.

[48] Giovanna De Maio, "Nel Baltico col fiato sul collo", in *AffarInternazionali*, 29 January 2015, http://www.affarinternazionali.it/articolo.asp?ID=2951; Andrius Sytas, "Worried about Russia? Lithuania says 'Keep calm and read the war manual'", in *Reuters*, 15 January 2015, http://reut.rs/1E2ALjq.

[49] Giovanna De Maio, "Nel Baltico col fiato sul collo", cit.

[50] Peter Apps, "Ambiguous warfare' providing NATO with new challenge", in *Reuters*, 21 August 2014, http://reut.rs/1wdWRzi; Alistair Scrutton e Sabina Zawadzky, "EU must prepare for Russia's 'hybrid warfare': Danish formin", in *Reuters*, 27 October 2014, http://reut.rs/1wvAhyU.

[51] Italian Army General Staff, *Linee di sviluppo evolutivo e innovativodello strumento militare terrestre*, cit., p. 26-27.

when intense fighting erupted between militias and rival governments. A scenario in which the Italian Army is called to intervene seems timely, in the light of the advance of the Islamic State and statements made by important members of the Italian government, who had suggested a peacekeeping mission in Libya within the framework of a United Nations' resolution.[52] In such contexts, the land conflict will feature several different dimensions, including the mediatic arena and cyberspace. Fights will take place in congested areas where it will be complex to discriminate between friendly or enemy forces and where it will be paramount to rightly choose between using force or not.[53]

3.2 The Italian Army and the netcentric capability

Recent modernization plans of several NATO countries' armed forces represent the latest example of the constant effort to incorporate new technologies in the military. As often in the field of military technology, the initial idea of a "netcentric capability" originated in the United States with the Network Centric Warfare (NCW) concept.[54] At the 2002 Prague summit, NATO countries took some important steps in this direction, when member states agreed to acquire a set of capabilities for "a digital transformation process." With the NEC (Network Enable Capability) acronym, NATO expressed the idea of "enabling the capability" of combining heterogeneous elements – doctrinal, procedural, technological, organizational and human – into a single network, in order to achieve, through the interaction of these elements, strategic superiority in military operations. It was a less radical approach with respect to the American NCW, but preferred by NATO, and particularly by countries such as France, Germany and Britain.

Italy firstly revealed its interest in the netcentric capability in the 2005 Chief of the Defence Staff Strategic Concept. The report stressed the im-

[52] Laurence Figa'-Talamanca, "L'Isis avanza in Libia. Gentiloni, pronti a combattere con Onu", in *Ansa*, 16 February 2015, http://ow.ly/2UGRdr.

[53] Interview, 4 February 2015.

[54] For further analyses see Michele Nones and Marrone Alessandro (eds.), *The Transformation of the Armed Forces: The Forza NEC Program*, Rome, Nuova Cultura, October 2012 (IAI Research Papers No. 2), p. 31-38, http://www.iai.it/en/node/1387.

portance of the "capability to gather, organize and share acquired data, by means of a robust net-centric C4I[55] system," to make the armed forces better suited to deal with future operations.[56] In 2006, the Defence General Staff (SMD) published the document "La trasformazione net-centrica: il futuro dell'interoperabilità multinazionale e interdisciplinare" (The Netcentric transformation: the future of multinational and interdisciplinary interoperability), in which the Chief of Defence, Admiral Giampaolo Di Paola, did no longer ask the question whether Italy should acquire or not a netcentric capability, but rather when and to what extent, recognizing it as an indispensable priority. Considering also the rapid evolution of armies' modernization plans in other NATO countries, the Forza NEC study program was launched in January 2007 as an inter-force program led by the Italian Army.[57]

The previous analysis of possible operational scenarios suggests that in the future the Army will continue to mainly operate in multinational peacekeeping operations. The operational experience acquired in theatres like Kosovo, Iraq, Afghanistan and Lebanon has been helpful in developing a series of specific TTPs (Tactics, Techniques and Procedures) and SOPs (Standing Operating Procedures) to conduct future operations in which the degree of interoperability among national armed forces will be key for success. It is in this context that the will of the Italian Army to acquire "NEC" needs to be considered.

For the Italian Armed Forces, the netcentric transformation means to be able to interconnect in a single

> network of 'sensors', namely technical or human elements which detect and survey natural and social activities, 'decision-makers', personnel who adopt a decision based on the information available, and 'actuators', weapons or soldiers that implement the decision taken. All these elements are integrated into a single structure, to

[55] Command, Control, Communication, Computer e Intelligence (C4I) represents the evolution of the command and control concept following the introduction of the Communications (TLC), Computer and Intelligence components.

[56] Italian Defence Staff, *The Chief of the Italian Defence Staff Strategic Concept*, 2005, p. 40, http://www.aeronautica.difesa.it/Missione/Documents/libroconcettostrategico.pdf.

[57] See Michele Nones and Marrone Alessandro (eds.), *The Transformation of the Armed Forces: The Forza NEC Program*, cit., p. 47.

> exploit synergies and operational capabilities to achieve effects which are coherent with the desired goals.[58]

In this sense, the digitization of the armed forces is the first step towards the realization of a netcentric system, that is the integration of tools and technologies into a C4I system to collect, exchange, correlate and use all the information obtained in the various stages of an operation.[59] The collection of information permits to acquire a Shared Situational Awareness, that is "the awareness of an operational situation among the forces."[60] By the means of a Shared Situational Awareness it is possible to gain the so-called "Information Superiority," which represents a force multiplier and a key element in achieving success, particularly in the context of joint and international operations.[61] In essence, the Netcentric capability offers the ability to integrate data in a unique Common Operational Picture (COP) and to provide a full overview of what is happening in the field. Knowing the course of events in real time is a major advantage as it allows commanders to make consistent and appropriate decisions according to developments on the ground, as well as adopting adequate counter and corrective measures. Through a sort of information fusion process, "Information Superiority" promotes better operations and mission management by commanders: an improved capability of target identification, classification and engagement; greater discrimination between allied and enemy forces; soldier protection from friendly fire; an effective integration of air and ground platforms; an improved logistics, planned according to the ground risks and threats. Digitizing also means to connect in a single network and to make communications possible among the different C2 systems used by the Armed Forces, and, possibly, their various assets, platforms and tools. In case of humanitarian intervention, the netcentric capability will allow the armed forces to improve communications in urban areas, to identify injured people and organize evacuation missions.[62]

The greatest advantage of embracing the netcentric philosophy would become tangible in multinational operations, allowing systems and struc-

[58] Ibid., p. 46.

[59] Ibid., p. 54.

[60] Ibid., p. 85.

[61] Ibid., p. 36.

[62] Ibid., p. 85-87.

tures of various countries' armed forces to communicate with each other in an automatic or semi-automatic manner. The undoubted benefit of this would be that troops operating in an international coalition would become completely interoperable. Interoperability is increasingly important in operations conducted in a multilateral context (NATO, EU and UN), and clearly, when achieved, it enhances the visibility of the Italian contribution to maintain peace, and might favour the direct assumption of command in specific missions when Italian interests are at stake.

Forza NEC is the foundation of a modern land force which is "expeditionary," "network capable," and "effect based operations-oriented," able to perform missions that reach the entire range of desired effects through the application of military, diplomatic, psychological and economic means.[63] During an operation, it aims to connect all the levels of the command and control chain, from the sensor (T0 level), to the soldier (T1 level), through all other intermediate levels: team (T2), platoon (T3), company/squadron (T4), battalion/group/regiment (T5), up to the brigade (T6). The netcentric evolution assumes that all systems are digitized, meaning equipped with new generation "networked" computer systems able to send and receive information and to communicate with each other according to specific policies of information management. Forza NEC acts as a catalyst for other procurement programs, providing both updates to other current programs or influencing the technical specifications of those not yet started. Forza NEC can be considered more than a mere procurement program because its outcomes will affect the broader modernization of the Italian Army. As an evidence of this, Forza NEC subsumes other programs like SIACCON, SICCONA, BFSA and the Future Soldier.

The SIACCON-2 (Automated Command and Control System ver. 2) is the C2 system used by the IA in fixed command posts (typically from battalion/regiment level and upwards) in support of military operations of various types. It is the evolution of SIACCON 1AW.

Similarly, the SICCONA (Command, Control and Navigation System) is the C2 system – used on ground combat platforms such as the VBM "Freccia," VCC "Dardo," Centauro etc. – providing command and control functionality, as well as data management of onboard weapon systems,

[63] Ibid., p. 54.

logistic (fuel, maintenance, spare parts, ammunition, etc.) and navigation information.[64]

The BFSA (Blue Force Situational Awareness) is a friendly forces identification system employed at tactical level and for navigation purposes. Unlike the SICCONA, it will be embedded on platforms not equipped with weapons and used for combat support and combat service support, as well as for logistics.

The Future Soldier program aims to equip the individual soldier with technologies improving its performances and transforming it in a network "node." The new concept behind the study of the Future Soldier System is based on the possibility to increase the soldier's protection, relying on the protection of each individual equipment components; avoid blue-on-blue (so-called fratricidal fire); and finally increase the overall effectiveness of the soldier. The program, in addition to the provision of standard non-NEC next generation equipment (helmet, bullet-proof vest, gun, modular backpack, pointing devices, individual safety kits, a new battledress, etc.) plans to equip the soldier with broadband radio and minicomputer to send messages with the other nodes of the network.[65]

As a further example, it is also possible to mention other equipment that will be updated: the Centauro armoured combat vehicle, the A-129 Mangusta attack helicopter, the Dardo armoured combat vehicle, the Freccia infantry fighting vehicle, remotely piloted aircraft systems (RPAS) and unmanned ground vehicles (UGVs) used for both attack and reconnaissance activities, the Light Multirole Vehicle (LMV) "Lince" and the Multirole Medium Tactical Vehicle (MMTV) "Orso."

[64] Compatibility between C2 and NEC assets and platforms is made possible due to a legacy solution called "Information Dissemination Mechanism." In the future, a "Service Bus" system is foreseen to be adopted. Interview, 10 February 2015.

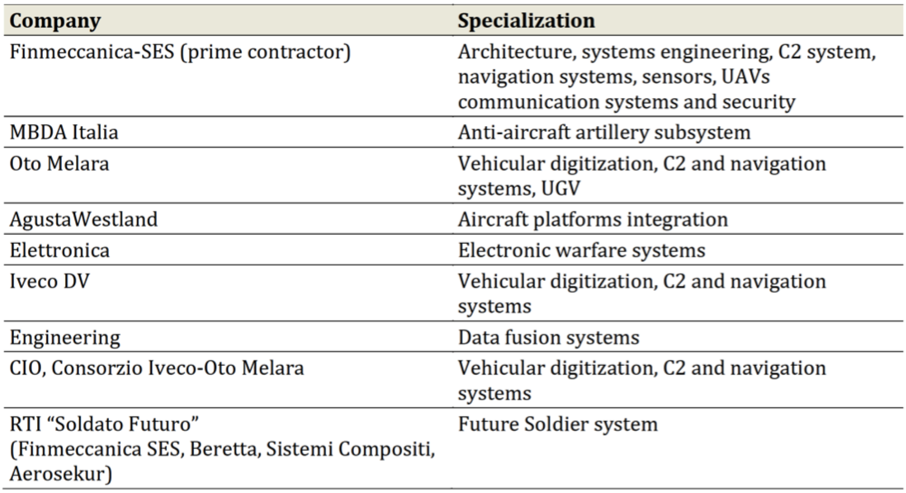
[65] One of the most important aspects of the program is the weight of the different "configurations" of the Future Soldier system, which is determined by the items/tools each soldier might carry: radio, night-vision viewer, minicomputer, cables and batteries. All electronic equipments weight between 4 and 5 kilograms, which is 15% of the weight a soldier can carry (a soldier should be able to sustain 1/3 of its weight). Since much of the weight a soldier might carry should comprise of ballistic protections, feed ration, arms and ammunition, the electronic component of its equipment should be the lightest possible to better allow soldier's mobility. Furtermore, special forces might be equipped with different systems, for example those employed for target's identification.

3.3 The industrial dimension of the Forza NEC program

3.3.1 The Forza NEC program

Forza NEC is a complex program aiming at the digitization of assets, platforms and tools in a single network. Because of this complexity, several specialized industries need to be involved in the project. Indeed, having several industries that do not coordinate their work would probably result in an inefficient process, and produce assets and platforms that at the end of the program might not be able to connect and communicate effectively with each other. Many companies operating in complete autonomy would also create additional pitfalls at the administrative and accounting levels, forcing the Ministry of Defence (MoD) to manage as many procurement contracts as the number of suppliers. To mitigate these risks, the Forza NEC program has introduced an interesting novelty, integrating in a single entity – the Finmeccanica-SES company – the roles of "system integrator" and "prime contractor." As a "system integrator," Finmeccanica-SES is responsible for ensuring the integration of components produced by other industries who take part to the program. In this way, the MoD does not have the technical challenge to assembly the various components of the NEC system by itself. The purpose of the system integrator

Table 1 – Companies involved in the Forza NEC program and their specialization



Company	Specialization
Finmeccanica-SES (prime contractor)	Architecture, systems engineering, C2 system, navigation systems, sensors, UAVs communication systems and security
MBDA Italia	Anti-aircraft artillery subsystem
Oto Melara	Vehicular digitization, C2 and navigation systems, UGV
AgustaWestland	Aircraft platforms integration
Elettronica	Electronic warfare systems
Iveco DV	Vehicular digitization, C2 and navigation systems
Engineering	Data fusion systems
CIO, Consorzio Iveco-Oto Melara	Vehicular digitization, C2 and navigation systems
RTI "Soldato Futuro" (Finmeccanica SES, Beretta, Sistemi Compositi, Aerosekur)	Future Soldier system

principle is therefore to ensure the coherent development of a "system of systems," integrating C2 systems, platforms and sensors in a unique architecture. Finmeccanica-SES is also the prime contractor, the only party the MoD has to interact with for the economic-administrative aspects of the program, acting as a coordinator among the other companies within the industrial consortium. Instead of interacting with diverse companies, the MoD liases with just one entity, possibly gaining clear benefits in terms of the linearity of the overall management process.

Forza NEC is an innovative program both for its governance structure and its management principles. Due to the extreme complexity of the program, its governance was subject to changes over the years. To date, the governance of Forza NEC foresees:[66]

- The Steering Committee, chaired by the Italian Army Logistic Commander, delegated by the Chief of Army Staff, which reports the results of the program development directly to the Chief of the Defence Staff. It includes the Department Heads of the Staff of the Defence, the heads of the Third Departments of the armed forces and the Secretariat General of Defence/National Armaments Directorate (SEGREDIFESA/DNA), through the Director of the Forza NEC program. The Steering Committee is responsible for providing strategic guidelines related to the development of the program and ensuring the achievement of the objectives, on the basis of the guidance provided by the Chief of the Defence Staff;
- The Project Office, chaired by the Head of Department for Terrestrial Transformation, focuses on the medium profile technical and managerial aspects of the program. The Project Office checks the program technical consistency and elaborates the programs' specifics to be developed in relation to the state of technological development reached by the industry.

In terms of management, the program follows three basic principles.[67] Firstly, it follows the so-called "capacitive approach." Already adopted at NATO level, the capacitive approach identifies the various assets to be

[66] Interview, 28 January 2014.

[67] Michele Nones and Marrone Alessandro (eds.), *The Transformation of the Armed Forces: The Forza NEC Program*, cit., p. 68-69.

acquired in relation to specific operational needs. According to this principle, the procurement program should identify tools, assets or weapons systems to meet past missions, but also future operational requirements. Secondly, the principle of "transforming while operating" states that upgraded systems need to be fully interoperable with systems that are not yet digitized. Finally, the cornerstone of Forza NEC, that is "evolution throughout production." The principle's goal is to keep systems and platforms updated with technological innovation. According to this principle, the systems to be upgraded are configured with an "open architecture," meaning that their structure is conceived to be further updated in the future. In short, the netcentric capability should allow different platforms to be reconfigured as technology advances.

3.3.2 Forza NEC phases and costs

Initially, the program was supposed to be completed in 25 years (from 2007 to 2031). However, the very nature of the financing, matched with a series of technical challenges, have significantly influenced the development and implementation of the program.[68] Originally, Forza NEC was organized in six phases:[69]

1. Feasibility Study (2007);
2. Project Definition (PD) Phase (2007-2010);
3. CD&E Phase (2010-2013);
4. First phase of implementation (within 2018): digitization of the first terrestrial digitized brigade (BIT), of the Landing Force (LFD) and of 50% of enablers; development of the Integration Test Bed (ITB) and of the Experimentation Phase through Modelling and Simulation (M&S);
5. Second phase of implementation (within 2026): digitization of the second BIT and of 25% of enablers;
6. Third phase of implementation (within 2031): digitization of the third BIT and of last quarter (25%) of enablers.

[68] So far, the Italian Parliament has funded only the so-called CD&E phase, not the overall program.

[69] Michele Nones and Marrone Alessandro (eds.), *The Transformation of the Armed Forces: The Forza NEC Program*, cit., p. 61-62.

To date, however the various phases of the program can be summarized as follows:[70]

1. Feasibility Study (2008);
2. PD (2009);
3. CD&E (2010 to 2020).[71]

After the feasibility study of the Forza NEC program, the PD phase began in order to: select the units to be digitized and the methods for their net-centric evolution; prepare the needed documentation to advance to the CD&E phase.

Differently from classic procurement programs, the CD&E, which is the current phase of the program, has been inserted between the PD phase and the industrial production of NEC platforms and systems. Given the complexity of the program, this step was added in order to mitigate the risks associated with the production of not yet tested systems. The objective of the CD&E is to produce a complete NEC architecture on a smaller and, through a series of tests, carefully evaluate the technological systems that will underpin the digitization of the Army. In other words, the CD&E seeks to produce the needed capabilities to "test and validate the architecture of the digitized force through the creation of all the main elements forming the NEC architecture on a small scale."[72] This stage has become somehow essential given the characteristics of the program, which seeks to digitize old assets and integrate them with ones. The AI and the industry have collaborated since the beginning of the program with the belief that the CD&E phase was also functional to build systems that would have then been "validated" in theatre. The CD&E has the scope to build five "macro" capabilities:

1. Digital C2: command post of the Task Force (brigade) of a digitized medium force including Command Control and Navigation (C2N)/ BFSA on LMV platform, third dimension (3D) C2N, development and upgrade of SIACCON and SICCONA;

[70] Interview, 4 February 2015.

[71] To date, 2020 is the most reliable estimate about the end of CD&E phase. Although contracts related to this phase could be closed as early as 2018, the production and testing of assets and platforms should last for at least two more years, until 2020.

[72] Interview, 28 January 2014.

2. Sensors: micro and mini RPAS, UGV (in different configurations); electronic warfare systems, Force Protection and Reconnaissance Surveillance and Target Acquisition (RSTA);
3. Actuators: development of Future Soldier's systems;
4. Communication and Information Systems (CISs): development of equipment for transmission of tactical data and ciphers; new generation satellite systems; gateway[73] for bidirectional connection of computer networks working at different levels of security and for the LFD; Software Defined Radio (SDR)[74] and the Battlefield Target Identification Device (BTID)[75];
5. Integration Test Bed (ITB): the ITB is the physical implementation of M&S, which is the set of activities that seek to faithfully replicate military units, platforms and weapons systems upgraded to the netcentric capability in a virtual mission scenario. Practically speaking, the ITB is an infostructure, consisting of hardware, software and buildings – connected with other ITBs – allowing to test all the elements of the netcentric capability. The virtual environments, set up in interconnected sites, employ a series of tools, i.e. simulation tools, to ensure communication among the centres and other networks. Given the joint nature of the program, these infostructures are not set up exclusively at the Army's headquarters, but also at Navy and Air Force facilities. Nevertheless, being the Army the main actor of the program, the main ITB site is the Centre for Simulation and Evaluation of the Army (CeSiVa). The CeSiVa and the ITBs of the Air Force and the Navy are connected in a single network to test the netcentric capability and to continuously exchange information. The ITB have had an impact not only on the experimentation phase, but also on soldiers training, due to the possibility of merging real and virtual approaches. The ITB significantly reduced the risk of the program's failure, and introduced a new way of working between the industry and the MoD personnel, who have been working side by side since its creation. The immediate effect of this approach was to ensure

[73] In telecommunications, a gateway is the node of a network used to connect with other networks using different protocols.

[74] Radio communication systems updated by software rather than hardware.

[75] Friend/Foe identification system.

> greater interaction between the two sides. That said, today the M&S is likely to be considered one of the program's elements of success, to be taken into account for future reference, in particular when it will be necessary to test pre-series instruments, structures and platforms or emerging technologies.[76]

To summarize, the CD&E phase:

- provides legacy platforms (e.g. Centauro, Dardo, Ariete), tools and systems with new netcentric features through which they can connect to the "network;"
- ensures the netcentric evolution of platforms that are new but already under production (e.g. VBM Freccia);
- conceives and tests future platforms and systems (New Centauro, LMV 2 MMTV, etc.) featuring a netcentric design.

Nevertheless, the very nature of the CD&E – a concept development and experimentation phase – has raised a few technical and administrative problems that have produced some delays, which, however, were expected by both the MoD and the industry. For this reason, the CD&E is now set to end by 2020, instead of 2013 as previously contemplated.[77]

First of all, some administrative/bureaucratic procedures aimed at verifying the full correspondence between the newly produced prototypes and the Army's initial requirements slowed the program down.[78] The very nature of the phase itself has almost inevitably produced delays, especially when a tool or a system, initially conceived only "on paper," had to be made compliant with some well defined operational standards before being tested on the ground. Furthermore, the integration under the umbrella of Forza NEC of a number of programs and contracts already in place generated an high number of intermediate contractual obligations ("milestones") delaying the process more.[79] In the end, the very same principles of management on which the program relies one, "transforming while operating" and "evolution through production," have sometimes caused overlaps between study phases, testing and evaluation, and

[76] Interview, 10 February 2015.

[77] Ibid.

[78] Interview, 4 February 2015.

[79] Ibid.

brought changes to the initial operational requirements. This has inevitably led to a slowdown of the CD&E phase. In particular, the principle of "evolution through production" – whereby the contract signed between the parties allows to change the operational requirements while the development of the new tools, systems and platforms is under way – seems to have put a considerable pressure on the pace and procedures of the industrial chain.[80] In other words, the pre-production phase had to bear into consideration continuous variations of specific TTPs and SOPs taking place while forces were in theatre, in addition to military technology's latest developments.

Besides administrative and bureaucratic constraints, other physical and technological limits have arisen, hindering the development of prototypes. The LMV and MMTV platforms are possible examples: the digitization of these platforms would have increased the weight and the number of equipment installed on board to the point of exceeding the capacity of the platform itself.[81] Similarly, the first prototypes of mini RPAS have proven resistant, but still too voluminous and heavy for being completely digitized. During the CD&E phase, some of the technological solutions suggested were not fully in line with the operational requirements sought by the armed forces, while on other occasion the timing of technological development did not allow to test the new generation platforms and systems in a shorter time. In general, it can be said that the typical problems of transitioning from an abstract requirement to a concrete solution have occurred, requiring changes along the way. The generation of the C2 software, for example, has raised many of the critical issues mentioned above. For commercial reasons, Microsoft has decided to switch from the Windows XP operating system to Windows 7, making the C2 software so far developed no longer supported – in terms of security updates – by the manufacturer.[82] Even with this in mind, and to prevent similar situations in the future, the industry has established a framework agreement with Microsoft to obtain early and timely indications on software's developments.

On the other hand, however, the CD&E phase has had two positive ef-

[80] Ibid.

[81] Interview, 10 February 2015.

[82] Ibid.

fects: the relationship established between the industry and the MoD and the identification of an initial set of systems/platforms/tools ready to be produced.

Regarding the first, the relationship between the MoD and the industry has allowed a fruitful exchange of information between the parties on the ground and during tests conducted by the Pinerolo brigade in Italy. Right from the beginning of the program, there has been a constant exchange of information between the parties in order to understand the major obstacles. As an example, the adoption by the industry of the new Agile Scrum methodology, which foresees the development of a software according to an iterative and incremental approach, as well as the direct involvement of the Army ("customer in the loop"), has drastically reduced the chances of failure in the development of prototypes.

Secondly, due to the latest developments of prototypes and pre-series systems, the CD&E phase has already identified those capabilities and systems ready for to be produced on a larger scale, bearing into mind that the overall success of the program – to be understood as the ability of all nodes to interconnect and exchange information – will be verified only at the end of the CD&E. Most of the main components can now be considered consolidated, namely the Future Soldier system, the SICCONA, the IPv4/v6 dual stack cipher and the digitized Command Posts (CPs).[83] With a reasonable degree of confidence, in the short term also some surveillance systems (UAV, UGV, and RSTA) will be ready, so other components of the digitized C2 system (the digitized artillery CP and the LOGBOX system for integrated logistics support), as well as some important CIS (the SATCOM On-The-Move (SOTM), the LFD Gateway and SDR radio equipment) in 2015.[84] A first general appreciation of the NEC capability was observed during the Italian participation to NATO's "Joint Eagle-Eagle Joker" exercise, in which ground vehicles, RPAS and mechanized units were connected with each other in a joint and multinational environment.[85] In addition, some of the capabilities considered ready will be deployed in exercise "Trident Juncture" in September 2015 in

[83] The Dual Stack allows the transition from the Internet Protocol (IP) v4 to the newest IPv6.

[84] Interview, 12 September 2015.

[85] Interview, 4 February 2015.

Spain, in the framework of the NATO Connected Force Initiative (CFI).[86]

In 2006, the total cost of the Forza NEC program was estimated by the industry at around 22 billion euros.[87] This estimate was merely tentative as it was made before the CD&E phase itself. Afterwards, the peculiar evolution of Forza NEC changed the way the program costs are considered for three reasons. The first one is that some of the technologies developed and tested in the CD&E have been later subsumed under other procurement programs with their own funding. Secondly, financially autonomous "spin off" programs were later launched to acquire technological solutions that had been tested in Forza NEC. Finally, the possibility of using the outcomes of the CD&E to influence the overall modernization of the Italian Army according to the NEC philosophy. All these elements will change the costs estimates of the program, especially since the CD&E phase is still ongoing. To date, the total cost of the Forza NEC program amounts to 815 million euro, including 15 million for the PD phase and about 800 million for CD&E phase.[88]

Given the research and technological implications, the program's costs fell almost entirely (except the 15 million for the PD) on the Ministry of Economic Development (MiSE), which funded the entire investment phase of CD&E.[89] Deemed essential due to the high-tech content of the program and the national industry's involvement, MiSE's funding gave relief, on one hand, to the already limited MoD's budget and, on the other, favoured investments in research and development (R&D) by the industry.[90] Funding from the MiSE has covered non-recurring costs associated with the Cd&E. Therefore, if the industrial production of the program's assets/platforms/tools will be free from such costs and will include only the recurring costs (i.e. the costs related to the mere industrial production of validated systems and assets).

[86] Interview, 10 February 2015.

[87] Michele Nones and Marrone Alessandro (eds.), *The Transformation of the Armed Forces: The Forza NEC Program*, cit., p. 61-62.

[88] The study phase was founded by the industry.

[89] Out of the 800 million euros foreseen for the CD&E phase, only 554 million have been allocated. Interview, 10 February 2015.

[90] Interview, 18 March 2015.

3.4 Forza NEC perspectives: challenges and opportunities

The Forza NEC program presents many challenges that, if positively faced, can turn into opportunities to be exploited in future procurements programs. Among these challenges/opportunities the main are:

- CD&E production of systems/platforms/tools;
- Armed forces education and training;
- Legacy assets;
- Joint interoperability;
- Tactical data management;
- Cyber defence.

CD&E assets production. The production of CD&E's systems/platforms/tools represents the real question mark of the program. The limited resources available to the MoD hinders any long-term planning ready-to-use systems, platforms and tools production. Despite this, from an operational but also financial and industrial point of view, the benefits to follow up with an industrialization plan are evident.[91] The acquisition of assets developed and tested during the CD&E phase should be considered in the context of the armed forces' comprehensive modernization plan. A minimal objective could be the acquisition of only those systems that are considered sufficiently ready to be compliant with the armed forces minimal requirements, and those which meet the armed forces' fundamental and minimal operational needs. Nevertheless, the IA should aim at gradually digitizing its systems through the production of "complete packages," which should include digital command and control systems, platforms and vehicles, sensors and soldier's equipment in order to equip at least a brigade. This should imply to hold the requirements and proceed to the production of a batch of digitized items. In the meanwhile, the experimentation and validation processes should continue at increasingly lower costs than those of the present CD&E phase (it would be focusing only on areas of greater technological innovation), in order to prepare the following batches at a higher technological level. In this way, it should be possible to reconcile, on one hand, the need

[91] Interview, 10 February 2015.

to acquire assets aligned with new technological standards and, on the other, the need to actually produce what has been created and tested during the CD&E. All of this would guarantee the delivery of the necessary assets to the IA and an adequate return on investments (ROI) to the industry. In the future, it could be appropriate "to freeze" basic requirements for an initial period agreed among the parties and to avoid changing the operational requirements in the experimentation and validation phases.[92]

Since the exact costs would be known only at the beginning of the phase following the CD&E, it would be necessary to take into account Italian government financial constraints, but also to provide the IA with the appropriate capabilities to operate within NATO. One should also recall the minimum spending requirements agreed by Italy (and by other allied partners) in the 2014 Wales summit – i.e. to spend at least the 2% of GDP on defence by 2024 – and its commitment to reduce the gap with the other main European countries.[93] While discussing what the Italian Army should acquire, one should also bear in mind the deterioration of the security conditions around Italy and to be part of an Alliance whose efficiency is related to the nature and quantity of the investments made in defence.

Armed forces education and training. The digitization process is a challenge for the whole Army organisation because it fundamentally alters the way soldiers are educated and trained.[94] The NEC capability allows obtaining information that needs rapid decision-making and critical thinking to be exploited. Because of that, military education and training should teach how to handle large amounts of information and to manage stressful situations in which soldiers face psychological and moral dilemmas. Training will need to realistically reproduce mission scenarios/events and prepare soldiers to cope with complex future threats, also considering the possibility to be deployed in theatres different from Afghanistan. With this respect, the land training system SIAT (Sistema Inte-

[92] Interview, 4 February 2015.

[93] In 2012, Italy spent 0.87% of its GDP on defence, as opposed to 2.08% by the UK, 1.49% by France and 1.2% by Germany. Roberta Maldacea, Alessandro Marrone, Paola Sartori, *Defence Budgets and Industry: Tables and Graphs*, July 2015, http://www.iai.it/en/node/702.

[94] Interview, 10 February 2015.

grato di Addestramento Terrestre) can ensure, together with the ITB, to adequately train the IA to the use of the netcentric capabilities.[95]

Legacy assets. Some challenges of the Forza NEC program stem from "structural" elements of the program itself, such as its extended duration and the technological complexity of the digitization process. As a matter of fact, to make the assets and systems of the IA netcentric, it was decided to upgrade to netcentric "standards" some of the vehicles and systems currently available, the so-called "legacy assets," while waiting for their replacement with new assets already designed according to the netcentric philosophy.[96] In other terms, it was decided to digitize what the IA already owns and to adapt it to the new netcentric capability. This process will lead to the implementation of netcentric capabilities in several phases, and not in a single one, as then stated in the Army Operational Concept 2010-2030 (Concetto Operativo 2010-2030 dell'Esercito) and in the Modernization Plan 2013-2030 (Piano di Ammodernamento 2013-2030). This process has been adopted in light of other countries' experiences, especially the US one.[97] As a result, during the Forza NEC CD&E phase, the Italian Army will own either updated systems, that will be replaced at the end of their operational life, or new systems with netcentric technologies already included.[98] At least in the current CD&E phase, legacy assets' issue does not seem to worry the industrial sector due to the intense prototyping process towards Netcentric technology that the main systems, assets and platforms have previously undergone. This pre-phase will allow the legacy assets to be compatible with the new technologies until they will be replaced.[99]

The potential obsolescence of new systems and platforms created and

[95] For a further analysis on the Italian armed forces training see Alessandro Ungaro, Alessandro Marrone and Michele Nones, "Technological Innovation and Italian Armed Forces Training: Challenges and Opportunities", in *Documenti IAI*, No. 15|02e, January 2015, http://www.iai.it/en/node/3247.

[96] Michele Nones and Marrone Alessandro (eds.), *The Transformation of the Armed Forces: The Forza NEC Program*, cit., p. 58-59.

[97] Indeed, the ambition and the costs associated with the Future Combat System (FCS) have compelled the Pentagon to review it and then develop it under the framework of the Army Brigade Combat Team program.

[98] Michele Nones and Marrone Alessandro (eds.), *The Transformation of the Armed Forces: The Forza NEC Program*, cit., p. 68-69.

[99] Interview, 4 February 2015.

tested during the CD&E is a potential source of concern because of the speed at which systems and tools recently produced will be no longer "new" due to technological innovations. To avoid this problem, during the testing and prototyping phases, systems and platforms should be configured according to an "open architecture," seconding rapid ICT technological developments.[100] In terms of hardware design, this means to take into account the platform's structure, its loading capacity and power supply in case additional systems will be developed and added in the 30-40 years lifecycle of normal platforms. If the industry was able to comply with the principle of "evolution throughout production" the replacement of new systems, assets and platforms currently under experimentation could be avoided. In order to keep pace with the constant technological evolution, a continuous experimentation phase would be paramount in order to evaluate the technical feasibility of further upgrading systems and assets which have undergone several digitization processes.[101] In this context, an important role will be assumed by "integrative batches" to level out and balance the different degree of technological innovation of assets, platforms and systems and to have, thanks to the ITB, a continuous "Experimentation and Validation Campaign of Capabilities."[102]

National and multinational joint interoperability. An additional technical challenge is to guarantee interoperability among the Italian armed forces at the end of the Army digitization process. In other terms, platforms and assets employed by the Army, the Navy and the Air Force must be able to communicate and interact with each other and also with those of other countries. Because the three armed forces do not employ the same instruments, not even the same C2 system, this is not an easy task. For example, the Italian Navy employs two different C2 systems, one at strategic (the Maritime Command and Control Information System, MCCIS) and the other at tactical level (Command and Control Personal Computer, C2PC). The Italian Army instead employs the SIACCON and SICCONA systems. The netcentric concept implies that the various C2 systems should be interlinked with each other, enabling the exchange of information among the network nodes, whether the node is a ship or a soldier.

[100] Interview, 10 February 2015.

[101] Ibid.

[102] Ibid.

The design and development of the netcentric architecture has envisaged specific components to support interoperability among national and international armed forces: at the strategic joint level, interoperability is guaranteed through the link between SIACCON and C2I (Command, Control, Intelligence) Difesa; at tactical level, instead, interoperability with the Navy is guaranteed through VMF messages and, in the future, through the Gateway of the Digitized Landing Force (GTWLFD), which should connect the C2 systems employed by the Army and the Navy (SIACCON-MCCIS and SICCONA-C2PC).[103] A greater integration with the Air Force will occur with the adoption of the CID (Combat IDentification) server, whose system is able to collect and correlate information on allied forces' position on the ground.[104] In turn, the CID server is interconnected with the Link 16, the Air Force communication system at tactical level, which allows units of several armed forces in theatre to exchange data in real time.

Within NATO, strategic-operational interoperability is supported by the MIP, a multinational program with the aim to define a common standard for data exchange among C2 systems. MIP is constantly tested both during joint international exercises and verified in periodic meetings on standardization procedures and techniques.

Tactical data management. The ability to connect a fair amount of nodes and make them communicate with each other is another important issue to be addressed, since the program aims to connect thousands of components. Forza NEC is fairly ambitious if one considers that the Navy and the Air Force, besides having started a digitization process earlier than the Army, have to connect at most few hundred ships or aircrafts. In fact, the Navy's fleets have already been connected with each other via data link for a long time, while the Air Force already conducts operations fully using the Link-16 system for data exchange, in compliance with NATO standards.[105] In other terms, the Army faces two problems: first, the Army starts from a lower level of digitization than the other two Armed Forces; second, it must connect an bigger number of elements in a

[103] Interview, 4 February 2015.

[104] Interview, 18 March 2015.

[105] Michele Nones and Marrone Alessandro (eds.), *The Transformation of the Armed Forces: The Forza NEC Program*, cit., p. 47-48.

network.[106] Once having solved this challenge, another issue is to process the huge amount of data originating from the nodes of the network. It is certainly true that the larger the collection of information the greater the possibility of achieving Information Superiority, but this will be useful only if an effective management of all the collected information is put in place. Working groups made of specialists from the MoD and the industry are currently working on specific solutions to overcome the problem. At this moment, the netcentric system foresees the presence of intermediate nodes that should be able to filter relevant information and send it to the higher levels (Regiment and Brigade) of the command chain. This is however a temporary solution. Software are being tested to "smartly" process data from the ground, meaning to collect information only from critical nodes, and thus avoid flooding the chain of command with irrelevant information. It seems clear that attention and efforts on this issue will focus more on the high levels of the command chain, because the chances of being adversely affected by an over-abundance of data is obviously greater at these levels.[107]

Cyber security. The Forza NEC program has been developed in a context strongly influenced by ICT developments. If the goal of the program is to achieve Information Superiority, a related issue pertains to the fact that collected data could be intercepted or the network tampered by enemies. Indeed, in a system with thousands of sensors, each "node" can represent an element of vulnerability. Against this backdrop, the "information security engineering" approach seeks to make systems more robust and resilient against possible cyber attacks. Security is further enhanced with "security hardening" activities, following assessment of information security systems conditions in the theatre of operations. Moreover, some innovative technological components such as the MILS (Multiple Independent Levels of Security) Gateway, have been designed to manage information between different domains depending on data level of classification. During the various simulations with the ITB, attempts have also been made to analyse and validate systems and platforms in terms of cyber security. Finally, encrypted internet protocols, which can manage classified data and can operate with devices that are based on different protocols, have been developed and implemented.

[106] Ibid.

[107] Interview, 18 March 2015.

3.5 Conclusions

This analysis on the interrelations between defence, industry and technology leads to some evaluations that are useful to put the Forza NEC program into a broader perspective.

Investing in defence technology is essential to ensure the strategic superiority that has characterized NATO countries over the past 25 years, both in crisis management operations and for deterrence purposes. The netcentric capability would enable Italy to continue having a high level of interoperability with the United States and other major European countries in multinational operations, such as those conducted in recent years, but also to face the emergence of a multipolar world, in which great powers like China and Russia could use "hybrid tactics" – or in some cases the use of conventional force itself – to achieve their political objectives. Recent international missions' objectives have often been achieved through superior naval and air power. This technological superiority has been realized through a process lasting several decades, in which investments and research allowed the industrial sector to effectively meet military requirements. Unlike the air and sea dimensions, where in the medium term Western forces will still enjoy strategic and technological superiority, in the near future the land component may find itself in more adversarial environments.[108]

One should also consider the impact that technologically advanced programs such as Forza NEC have on the rest of Italian industry. The development of advanced systems often has positive effects in fields other than the military, such as command posts or UAVs, which are dual-use technologies stemming from the Forza NEC program. At the same time, advanced systems developed for the IA might be exported to allied or friendly countries and yield significant economic returns for the Italian industry. These economic gains will be crucial to maintain a competitive industrial base despite the limited funds allocated by the Italian government on defence. Some concrete and positive "spillovers" of the program are already evident, such as the Oto Melara UGV, the Iveco LMV-2 or the Finmeccanica-SES SDR radio.[109] The Forza NEC is certain-

[108] Italian Army General Staff, *Linee di sviluppo evolutivo e innovativo dello strumento militare terrestre*, cit.

[109] Interview, 4 February 2015.

ly a complex program, but whose experimentation and testing phases really permit a qualitative leap forward of the industry. Moreover, the ability to develop new solutions and to compete internationally with other countries are useful to mature a remarkable comparative advantage, encouraging exports to emerging markets and the spread of a high quality Italian brand. Technological development should, however, be supported by a coherent investment plan to continue honing the technological and industrial expertise acquired after years of research and development. Having an industry capable of developing advanced technological solutions also responds to the need of maintaining sovereignty over systems, platforms and infrastructures. This will inevitably play a role in a possible and desirable process of European defence integration, in which the contribution that each country will provide will be determined by the level of technological competitiveness to be shared with partners.[110]

In the light of the current policy that has repeatedly asserted the need to "do more with less," the modernization of the land component becomes crucial.[111] The Army, like the other armed forces, is under pressure due to the attrition of equipment in last international missions and the lack of economic resources. Limited funding is affecting the overall renewal of the defence sector, including the acquisition of technologies, personnel training, and maintenance of vehicles. In the last decade, the Italian Army has relied on 60% of the funds that would have been needed for the modernization of the armed force.[112] Investments in technology would allow to replace assets worn out by operations, to better manage resources and to protect soldiers in theatre.[113] Moreover, given the changing international security context, it would be an even greater mistake to object further investments in technology. Consequently, what is now a reality – a close collaboration between the industry and de-

[110] Italian Army General Staff, *Linee di sviluppo evolutivo e innovativo dello strumento militare terrestre*, cit., p. 65.

[111] Italian Ministry of Defence, *Tecnologia e innovazione per la difesa europea. Pinotti: fare di più con meno la nuova sfida globale*, 11 July 2014, http://www.difesa.it/Primo_Piano/Pagine/20140711_ConvegnoAvioAero.aspx.

[112] Italian Army General Staff, *Linee di sviluppo evolutivo e innovativo dello strumento militare terrestre*, cit., p. 16.

[113] Ibid., p. 17.

fence sectors working side by side from the beginning of a program – will hopefully be consolidated in the future and allow Italian armed forces to be in line with the innovation of other foreign armed forces, keeping costs on a sustainable track and with the perspective of sharing efforts with the EU and NATO.

4. The Challenges of Netcentric Capabilities

Alessandro Marrone, Michele Nones and Alessandro R. Ungaro

Nowadays, it seems prosaic to remind how the Information and Communication Technology (ICT) has completely transformed the economy and the same societies of the Western countries and, to a certain extent, of the whole world. It seems prosaic because we get used to the permanent flow of information between a huge quantity of different and physically distant devices through the network – computers, TVs, tablets, smartphones, etc. – and we get used to their growing speed in processing and integrating data, destroying the barriers among textual, video and audio formats. All this takes place at an exponentially increasing connection speed, while the devices miniaturize themselves and the interfaces become more and more customized denoting needs and desires of every single user.

On the other hand, it is less prosaic to gather the direction and the pace of the transformation introduced by ICT. By now, in both the academic and non-academic environment, it is not possible anymore to talk only of "third industrial revolution," which happened in the '80s and '90s with the ICT, but also of a "fourth industrial revolution" or even of "Industry 4.0."[1] The new frontier is the Internet of Everything (IoE), a further step forward the so called Internet of Things: IoE is based on a new technological infrastructure combining network of sensors for personal usage and/or incorporated in objects, products and other things with the wire-

[1] See Andrea Renda (ed.), *Global Outlook 2015: rapporto finale*, Rome, IAI, 29 April 2015, p. 92-100, http://www.iai.it/en/node/4141.

less connection, rendered intelligent as sources of new data and information, and put under disposal for the development of a new systems' and services' ecosystem.[2] It is estimated that the number of the connected devices in the global network will pass from 13 billion of 2015 to the 50 billion of 2019.[3] This lays on progresses in the cloud, in the robotics, in the sensors, in the big data management, in the satellite communication system, in the microprocessors, etc.[4]

It is not only a technological revolution, but also a revolution of the forma mentis and of the modus operandi of those who use the ICT not only in their own working life, but also in their public and private one: in fact, it is about reasoning in a more horizontal than vertical way, more exponential and less linear, considering the past not as a burden, but as an heritage to be rebuilt over new bases. In the "disruptive technologies"[5] modern age it is foreseen that by 2027 the 75% of the 500 big companies in the Fortune's rank will be replaced by new realities not currently present in the rank yet: briefly, for a big company – and not only – the option is to be "disrupting" or "disrupted."[6]

These brief considerations clearly specify that the technological, industrial and economic progress aims at the digitization and the connec-

[2] For a broader understanding of the topic, among the others, see: Camilla Bellini and Elena Vaciago (eds.), *Internet of Everything: stato dell'arte, trend evolutivi*, Milan, The Innovation Group, June 2014, http://www.theinnovationgroup.it/?p=21936.

[3] Andrea Renda (ed.), *Global Outlook 2015: rapporto finale*, cit., p. 92.

[4] See, among the others, "Of robots and men", in *Aspenia*, No. 68-70, December 2015.

[5] In their article of 1995, became quite known ("Disruptive Technologies: Catching the Wave", in *Harvard Business Review*), Joseph L. Bower e Clayton M. Christensen talk about "disruptive" technological challenges. "Disruptive technologies" mean the specific technologies initially supporting those largely tested and diffused without apparently threatening the existence, but these are aimed for new categories of customers radically redefining the ecosystem and the role of the enterprises in this productive ecosystem, thus forcing the strengthened industrial actors to revise consistently their own plans and business models. For instance, Umberto Bertelè from the Politecnico of Milan meditates over the fact that there is the tendency to buy ever less compact digital cameras "not because someone wants to substitute Canon or Nikon, but because the smartphones offer the same feature at a quasi-null perceived cost and at a qualitative level that continues to grow as a consequence of the war among smartphones' producers." Cfr. Umberto Bertelè, "Le opportunità della disruptive innovation", in *ICT4Executive*, April 10, 2014, http://t.co/pQaNigcrix.

[6] IAI Global Outlook seminar, Rome, 26 March 2015.

tion, with a ripple effect over all the social life's aspects, included the military environment that cannot be excluded from dealing with the ICT.

With such a revolution, partially occurred and partially still ongoing, it is necessary to value if, how and how much the Italian armed forces – and the armed forces of the main NATO countries – are able to take the opportunities offered by ICT and to manage the risks linked to them. In doing it, a good dose of realism and understanding of the specificities of military environment is needed.

Generally, public administrations, included the armed forces, are less flexible, innovative and quick than the subjects belonging to the private sectors, not because of a minor quality of their own human resources, but for their different planning, structure and way of working. In fact, the public sector has the duty of taking decisions and acting through extremely formalized procedures, often complex and rarely quick ones. This condition tends to reduce the leeway for the leadership to perceive the innovation (technological and organizational), increasing the time and the resources for the procedural aspects of every activity.

This is particularly true for public contracts, a category in which the military procurement is included. Furthermore, the system of incentives and disincentives in the public administration usually penalizes the assumption of risk, which is basically linked to an innovation process, and it encourages in a more or less indirect way the preservation of the status quo.

In this context, the armed forces are not an exception. Due to their peculiarities, they face with further limits in the approach with the ICT. First of all, for its nature the military instrument is aimed at using the strength to force the enemy to accept its own political will.[7] Thus, there is an enemy who opposes himself with all the possible means, symmetric or asymmetric, to the action of the armed forces, and this contributes to create a sort of "friction" that makes every operation more difficult, risky, complex, and in some cases disastrous.

It is not by chance that within the military operations, from the counter-guerrilla to the peace-enforcing and peace-making missions, from the

[7] The definition owns to Karl Von Clausewitz, and it is combined with the well-known Clausewitz's definition of war as "prosecution of politics by other means." See Karl Von Clausewitz, *On War*, New York, Oxford University Press, 2006.

counter-terrorism activities to hybrid warfare, up to the hypothesis of an interstate war,[8] lasts the uncertainty and the risk over the behaviour and the result of operations – the so-called "fog of war."[9]

In the same way, it is possible to affirm that also the companies face the will of their own competitors to prevail over the market, and that the private sector is normally exposed to many kinds of cyber-attacks.[10] Nevertheless, the two field are not comparable. The economic intelligence, nowadays largely applied also through cyber intrusions, can lead to the acquisition of adversary's know-how and thus to a partial advantage in industrial terms. However, no private subjects look to completely cancelling the internal communication system of a competitor in order to then destroy physically its assets – as happened in 1991 and 2003 to the Iraqi armed forces, and in 2011 to the Libyan ones, after the destruction of its own command and control systems by the Western coalitions.

In the military field, the life of soldiers is directly at stake, and this entails specific necessities and requirements for the ICT: while in the civilian environment it can be possible to possess an extremely performing smartphone, even if with a battery lasting few hours – because there will be time and way to charge it every day – the same is not be said for a platoon during patrol mission or for a special forces task force in action in Afghanistan: both of them cannot allow the loss of radio contact because of the depletion of the batteries.

The computerized devices must respect the maximum standards not only in cyber-security terms, but also in terms of countermeasures for the electronic war, and at the same time these will have to have hardware and software able to operate in adverse environmental and operational conditions.

[8] Not remote hypothesis neither for the Italian military instrument, which fought the Iraqi Armed Forces in 1991, the Serbian ones in 1999 and the Libyan forces in 2011, in the context of international missions besides Western allies, but always in a substantially inter-state war.

[9] See Karl Von Clausewitz, *On War*, cit.

[10] The statement of the president and managing director of Cisco John Chambers is essential and efficient: "There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked." John Chambers, "What does the Internet of Everything mean for security?", in *World Economic Forum* blog, 21 January 2015, http://wef.ch/1C8yELC.

Thus, the armed forces find themselves in a unique and extremely difficult situation. On the one hand, the technological revolution of the ICT has changed and will continue to radically change the economy and the society at a global level, and so the reference frame in which the enemies and the allied operate.[11] On the other, the armed forces face with a series of structural limits, because they are part of the public administration and part of a conflict, in keeping opportunities offered by the ICT and to manage the risks coming from it. Facing the same problems, the US and European armed forces have tried to find similar solutions and different ones based on the specific national realities.

In the United States the ICT and the netcentric capabilities became deeply and irrevocably rooted in military operations, especially in the light of the so called "lessons learned" emerged during the Iraqi and Afghan wars. What seems making distinguished the American approach, compared to that of other states technologically and military advanced, it is the double verification of the huge potentialities and of the significant vulnerabilities of an increasing entrustment to a complex networks' system at the basis of the netcentric capabilities.

The will of developing the usage of such capabilities in each of the six "combat functions" – C2, Intelligence, Fire, Movement and manoeuvre, Protection and Support – shows how the US military establishment is deeply aware of the necessity to continue towards a complete "networking" of the physical and human assets that shape the armed forces.

At the same time, assuring the integrity of networks and of the information going through them is ever more a key issue within the US debate. Every single domain within the US joint doctrine – air, land, sea, space and cyber – plays a fundamental role in order to facilitate the employment and the usage of netcentric capabilities. For these reasons, the interests and the financial efforts made by the US military are especially oriented towards the neutralization or the attenuation of the main threats that could cause a possible interruption of the networks – such as cyber-attacks, "congested" electromagnetic spectrum and growing quantities of spatial

[11] Nowadays, Google Earth offers to every group of rebels linked to internet the possibility to have an idea of the geography of the best operational theatre compared to the idea of the Allied General Staff had in 1944 during the planning of the landing at Normandy, or the Israeli Army when it crossed the Suez Canal during the Yom Kippur War in 1973.

debris. In particular, the electromagnetic spectrum and the extra-atmospheric space concern quite a lot the US armed forces. For instance, it could be possible to mention the continuous efforts to develop a specific defence system from the electromagnetic pulses and the information sharing agreements stipulated by Washington with commercial companies and other governments having PNT capabilities in order to ease the US access in case of damage or involvement of its own.

As every radical technological revolution that has to find its application in the military field, also the path towards the netcentric capabilities is not excluded by obstacles and difficulties, at both technical-engineering and political level. Except some specificities connected to the US reality – as certain institutional, legal and financial issues – the armed forces of the United States face the same necessity to overcome physical limits inhibiting the real range of netcentric capabilities. In particular, it refers to those restrictions currently imposed by technology, as in terms of weight, seizes and strength of systems through which equipping the soldiers, and that are under observation of specific programs of R&D aimed at researching new solutions to "release" the potentialities, as yet remained partially unexpressed and unexploited, of the netcentric capabilities.

At the same time, the joint interoperability, and especially with the main allied countries, still remains an aspect that – beyond the rhetoric and some isolated example – seems missing true operative concreteness, maybe because of the lack of a real political will of establishing a solid and structured cooperation to this purpose. The uncertainties over the amount of the defence budget and the financial restriction already experimented in the past years have led the US armed forces to prefer initially a more "domestic" approach. Such an approach gives priority to the resolution of internal problems, and only after having reached an adequate level of joint interoperability is possible an orientation towards a multinational and of netcentric integration perspective with the other assets and platforms belonging to the main partners' armed forces.

In the Old Continent, the starting point and the ambitions in the field of netcentric capabilities are partially different. France, Germany and United Kingdom have undertaken their own path for the netcentric transformation of their respective armed forces, which has been influenced also by the experience in the international missions of the last fifteen years. For example, France quickly undertook the digitization of the single soldier's level – with the program FELIN – and it could develop the process in a vertical way without pressure of operative duties as the one in Iraq and in Afghanistan. Instead, the United Kingdom had to turn to the UOR for equipping its own brigades massively employed in the Iraqi and Afghan theatres, often acquiring equipment off-the-shelf by different suppliers and thus aggravating the networking of the assets and the construction of a netcentric architecture – without considering the drainage of resources from the ordinary procurement programs towards the support of the UOR. Germany placed in a mid position compared to the French and British extremes, with a certain coherence in the commitment for the digitization of its armed forces and, simultaneously, a significant military and prolonged strain in Afghanistan (but not in Iraq).

As regards the threat to the network, the cyber-security gained ever more importance within the British and French conception. Both the armed forces are developing capabilities not only of cyber defence but also of attack, as compensation for the identified vulnerability linked to the digitization process of the respective armed forces. This commitment is followed by a certain activism of defence industry in the two countries. Germany has also moved in this direction, even after the recent crisis in Ukraine, in particular for what concerns the capabilities of early warning and interdiction towards cyber-attacks.

In term of C2, the British case of the architecture of communication at a tactical level Bowman is a good example of the difficulty for the armed forces at keeping up with the technological innovation in the ICT field. The Bowman system started to work in 2008 after a long gestation phase because of the complexity to digitize and network the Army's assets, and since 2015 a more updated version is being introduced. Yet already in 2018 is foreseen the substitution of the Bowman system with a new one, also known as Morpheus, which should be more easily updating in the time to keep up with the ICT developments. In France, the program SCORPION uses a centralized approach to the acquisition of vehicles, weapon and communication systems in order to obtain netcentric capabilities. Although, the upgrade of the current communication architecture, the SICS, is simultaneously financed to maintain operative the vehicles that will not be reconfigured within the SCORPION. The merge of the two programs aims to balance the need of keeping up with the ICT together with the impossibility of replacing tout court the asset legacy of French Army. Even Germany had to face similar problems. The digitization program IdZ of the single soldier's equipment – the equivalent of French FELIN – started in 2004 but it saw the delivery of the first stock only in 2012. The fact that the vehicles of the German Army are new or in phase of acquisition is a positive factor due to the fact that these are already designed to satisfy the netcentric requirements.

Generally, a more cautious approach has been adopted in all the three countries if compared to the United States. This happened also because of the budget limits and/or of the short-term needs linked to the ongoing operations. Nevertheless, they recognized the importance of the netcentric capabilities, in particular of the cyber field, investing huge economic resources in facing the difficulties generated by netcentric transformation in terms of asset legacy, interoperability and obsolescence of acquired systems.

It is in this context that the Italian experience has to be evaluated. The same cautious and progressive approach to the netcentric transformation of the Army was needed also to face the intrinsic difficulties of the armed forces in exploiting the opportunities of ICT and mitigating the risks.

It is not by chance, as happened for example in France, that Italy chose to update part of the asset legacy to the netcentric standards and to still maintain it in service for long, waiting that the equipment were substituted by new assets that are able to incorporate the netcentric technology in the design phase. The problem of the brigades operating under "different technology" is thus a reality with which it will be necessary to coexist. The only way to go towards the netcentric capabilities is to forecast and manage an interrupted phase-in cycle of new platforms closer to the highest performances in terms of ICT, in replacement of one part of the asset legacy and, simultaneously, to identify the remain part of the asset legacy more convenient to update.

In this case, in order to follow a more advanced technological solution, the armed forces utilize more obsolete equipment, while what is being developed will never be applied in the operative theatre because of its further continuous updates. This risk is strictly linked to the principle of the "evolution through production," and it can be avoided by a realist approach that prefers a usable solution in a short time though not perfectly at the maximum levels, combined with the use of the “open architecture” in order to later upgrade the system gradually introduced.

The other risk of this path towards netcentric capabilities is that of surrendering – *de facto*, if not officially – in front to the aforementioned difficulties in developing advanced technologies to remain anchored to bureaucratized procurement procedures, low efficient and effective (and also inappropriate to CD&E). On the other hand, the more suitable and convenient path to follow is instead the one that foresees to “fix” the new systems/sensors/devices verified by technical-tactical tests over operative prototypes and starting the series production aimed for equipping as much the single fighter as the whole units. By keeping this path, the benefits of the research and development could be reaped and the renovation of at least a part of the armed forces elements could be carried out by gradually and increasingly proceeding in the future in terms of technological innovation with developmental and modular approach.

After the natural and physiological drawbacks and delays, the results produced during the CD&E phase of the Forza NEC currently allow the implementation of technical tests and tactical trials of integration on more levels and from a joint perspective. These “campaigns” with the Pinerolo Brigade and the Experimental Unit of Digitization conducted with the industry confirm the possibility to achieve concrete goals, comparable to those of the main European countries with which Italy measures itself and cooperates at political, military and industrial level. In this context, the interoperability, the management of the data in the theatre and the cyber security issues must be considered. The excessive attention of each armed force for its specificity is a further element that makes the netcentric transformation difficult, in particular by limiting and posing obstacles to the joint interoperability at tactical, operational and strategic level. The management of huge data flow, as that resulting from the networking of thousands sensors of the many units of the Army, is a particularly complex activity for the armed force. In fact, in a hierarchical structure as the military, it is necessary that information is vertically shared, but this represents the double problem of not obstructing the chain of command with a big quantity of irrelevant data, and of avoiding the risk of micro-management once the superior levels are able to access real time to the same information of the inferior ones and of communicating as much quickly their own orders. Not a new problem for the armed forces but not for this less relevant for an effective management of the military operations.[12]

For what concerns cyber security, it stands as a priority not only for the United States, but also for the main European countries. It is possible to understand the efforts of the Forza NEC program in this field, from the "security hardening" activities to the simulation conducted through the ITB. Nevertheless, it is necessary to be aware that in the cyber domain the competition between "attack" and "defence" proceeds to an exponential speed compared to the one experimented throughout the past centuries in the military context, the so-called "sword-shield" or "armour-cannon" dynamic that assumes a reinforcement of the defensive capabilities if the attack ones are strengthened, and vice versa. Therefore, this eternal competition deserves attention and constant investments, in order to maintain the vulnerability of a military instrument at acceptable levels.

Compared to the cyber security, and more generally to the netcentric capabilities, it is fundamental to reflect about the importance of technologies within the military field. Throughout the modern and contemporary history, the technological innovation has often given the impression to have the ability to provide the "strategic" or "definitive" weapon, decisive in every conflict, as in the case of the "air power" theorized by Giulio Douhet between the Great War and the arrival of the atomic bomb at the end of the Second World War.[13] Nevertheless, every time, the union disposed of the same technological innovation and especially of the challenges in the ways of military operations' management tactically, operatively and strategically, have compensated the relative advantage given at a first moment by the new technology utilized for military purposes.[14]

[12] When the telegraph exponentially accelerated the communication through the C2 chain of the European armies, the German and French Armed Forces exploited in a different way the potentialities offered by the known technology at the eve of the Second World War: while Germany let large autonomy to the commanders of the divisions involved in the operational theatre, according to the Blitzkrieg doctrine, French maintained the same dependence of the deployed forces along the Maginot Line by the Paris command, and this contributed in a substantial way to the French defeat in 1940.

[13] In the article "I problemi della aeronavigazione" published in the magazine *La Preparazione* in 1910, and then in his most famous book of 1921, *The Command of the Air*, http://www.au.af.mil/au/awc/awcgate/readings/command_of_the_air.pdf.

[14] See Edward N. Luttwak, *Strategy. The Logic of War and Peace*, Cambridge, Belknap

In this context, even the ICT is not an exception, and therefore the advantage assured by the netcentric capabilities has to be commensurate with the enemy’s ability to modify his own strategy to compensate the disadvantage in which it finds itself: friction and risk cannot be deleted nor by a full “information superiority” nor by the best “situational awareness.”

In other words, the technology is not and cannot become the solution to every security dilemma, because the operative environment will be still characterized by the human dimension. Notwithstanding that the improvements obtained in the military context are undeniable thanks to the technological innovation, and in particular thanks to the ICT, it is necessary to be aware of the limits of an excessive entrustment on advanced systems. For instance, aware of the Western governments’ attention to the national public opinion, the adversaries have often applied asymmetric tactics against the technological superiority of NATO countries, using propaganda or terroristic means, and using the population as a shield against the attacks coming from the most advanced armed forces aimed at undermining the internal consensus for the military intervention. Even other different state realities extensively use means of disinformation and intimidation, as well as of non-state actor, in order to pursue own objectives in what today it is called “hybrid warfare.”

Only the technology can barely prevail over the human aspect of the conflict in the moment in which adequate measures are not taken to face with it. In this regard, Italy, and generally the Western countries, will have to assure to be able to conduct military but also political fights, and to be able to integrate their own military and civil assets in a more coherent and synergic way. If it is true that technology itself is not sufficient to achieve military objectives of a country such as Italy, it is also true that it is absolutely necessary – a real condition sine qua non. In particular, today and in the near future the netcentric transformation of the military capabilities represents an undeniable transition in order to maintain the efficiency and the validity of the armed forces, especially of the Italian Army.

Press, 2001.

Bibliography

Army Science Board, *Decisive Army Strategic and Expeditionary Maneuver*, 18 September 2014

Camilla Bellini and Elena Vaciago (eds.), *Internet of Everything: stato dell'arte, trend evolutivi*, Milan, The Innovation Group, June 2014, http://www.theinnovationgroup.it/?p=21936

Umberto Bertelè, "Le opportunità della disruptive innovation", in *ICT4Executive*, April 10, 2014, http://t.co/pQaNigcrix

Joseph L. Bower e Clayton M. Christensen, "Disruptive Technologies: Catching the Wave", in *Harvard Business Review*, Vol. 73, No. 1 (January-February 1995), p. 43-53

Bob Brewin, "Army Eyes 4G Cellular Tech for Combat Communications", in *Nextgov*, 10 September 2014, http://www.nextgov.com/defense/2014/09/army-eyes-4g-cellular-tech-combat-communications/93689

Bob Brewin, "The Navy wants a tactical cloud", in *Defense One*, 25 September 2014, http://www.defenseone.com/technology/2014/09/navy-wants-tactical-cloud/95129

Nick Brown, "Airbus adds internet freedom to UK TACIP", in *Jane's International Defence Review*, 26 November 2014

Carl H. Builder, Steven C. Bankes, Richard Nordin, *Command Concepts. A Theory Derived from the Practice of Command and Control*, Santa Monica, RAND, 1999, http://www.rand.org/pubs/monograph_reports/MR775.html

Amy Butler, “USMC to outfit Ospreys with comms node”, in *Aviation Week & Space Technology*, 14 October 2013, http://aviationweek.com/node/4026

Vincenzo Camporini et al., *The Role of Italian Fighter Aircraft in Crisis Management Operations: Trends and Needs*, Rome, Nuova Cultura, March 2014 (IAI Research Papers No. 16), http://www.iai.it/en/node/2155

James Jay Carafano and Richard Weitz, “EMP attacks: What the U.S. must do now”, in *Heritage Foundation Backgrounder*, No. 2491 (17 November 2010), http://www.heritage.org/research/reports/2010/11/emp-attacks-what-the-us-must-do-now

Edward C. Cardon, *Keynote Address*, Brookings Fifth Annual Military and Federal Research Symposium: “Securing America’s Future in the New ‘Interwar Years’”, 12 March 2014, http://brook.gs/1F8BpAi

John Chambers, “What does the Internet of Everything mean for security?”, in *World Economic Forum blog*, 21 January 2015, http://wef.ch/1C8yELC

Karl Von Clausewitz, *On War*, New York, Oxford University Press, 2006

Fabrizio Coticchia, *Qualcosa è cambiato? L’evoluzione della politica di difesa italiana dall’Iraq alla Libia (1991-2011)*, Pisa, Pisa University Press, 2013

Giovanna De Maio, “Nel Baltico col fiato sul collo”, in *AffarInternazionali*, 29 January 2015, http://www.affarinternazionali.it/articolo.asp?ID=2951

Nadia Deseilligny, “France earmarks EUR1 billion in spending on cyber defence”, in *Jane’s Defence Industry*, Vol. 31, No. 2 (1 February 2014)

Justin Doubleday, “Army aims to jump-start development of radio-frequency defenses”, in *Inside the Army*, 29 December 2014

Justin Doubleday, “Army crafting career field, occupational specialty for cyber forces”, in *Inside the Army*, 19 September 2014

Justin Doubleday, "Army seeks info on Patriot-interface kits for networked missile defense", in *Inside the Army*, 3 October 2014

Justin Doubleday, "Congress approves Army funding for 'assured' navigation technology", in *InsideDefense.com*, 10 October 2014

Justin Doubleday, "Solicitation eyed this fall for 'unified capabilities' networking tools," in *Inside the Army*, 19 September 2014

Giulio Douhet, *The Command of the Air*, 1921, http://www.au.af.mil/au/awc/awcgate/readings/command_of_the_air.pdf

Giles Ebbutt, "Beyond Bowman", in *Jane's Defence Weekly*, Vol. 51, No. 26 (25 June 2014), p. 28-31

European Defence Agency (EDA), *Progress for European Satellite Communication Procurement Cell (ESCPC)*, 5 February 2014, https://www.eda.europa.eu/info-hub/press-centre/latest-news/2014/02/05/progress-for-european-satellite-communication-procurement-cell-(escpc)

Jesse Ellman, Gregory Sanders and Rhys McCormick, "U.S. Department of Defense Contract Spending and the Industrial Base, 2000-2013", in *CSIS Events*, 16 October 2014, http://csis.org/node/52055

Sydney J. Freedberg, "The Army gropes toward a cultural revolution", in *Breaking Defense*, 22 October 2014, http://breakingdefense.com/?p=16597

Sydney J. Freedberg, "STRATCOM lacks authority, $$ on electronic warfare", in *Breaking Defense*, 7 October 2014, http://breakingdefense.com/?p=16291

Sydney J. Freedberg, "What the US, NATO must do to counter Russia: Breedlove, Gorenc & Odierno", in *Breaking Defense*, 22 September 2014, http://breakingdefense.com/?p=15930

German Ministry of Interior, *Cyber Security Strategy for Germany*, February 2011, p. 2 and 3, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf

Matthew Glavy, "The Flight MAP: The Marine Aviation Plan Through 2040", in *CSIS Events*, 28 April 2014, http://csis.org/node/48793

Mikhail Gorbachev, "A New Cold War Order", in *Project Sindicate*, 5 January 2015, http://po.st/QpXoPk

Joe Gould, "New war game to focus on tech, partnerships," in *Defense News*, 13 October 2014, http://www.defensenews.com/article/20141013/SHOWSCOUT04/310130030

Mary-Louise Hoffman, "Heidi Shyu: Army eyes interoperability, open standards for ground robotic system", in *Executive Gov*, 15 August 2014, http://www.executivegov.com/?p=62462

Mike Hoffman, "Marines Work to Extend K-MAX in Afghanistan Through 2014", in *DefenseTech*, 25 September 2013, http://defensetech.org/2013/09/25/marines-work-to-extend-k-max-through-2014

Italian Army General Staff, *Linee di sviluppo evolutivo e innovativo dello strumento militare terrestre – PROSPECTA*, 2015

Italian Defence Staff, *The Chief of the Italian Defence Staff Strategic Concept*, 2005, http://www.aeronautica.difesa.it/Missione/Documents/libroconcettostrategico.pdf

Italian Ministry of Defence, *Linee guida del Libro bianco per la sicurezza internazionale e la difesa*, June 2014, http://flpdifesa.org/wp-content/uploads/2014/07/Linee-Guida-per-il-Libro-Bianco.pdf

Italian Ministry of Defence, *White Paper for International Security and Defence*, July 2015, http://www.difesa.it/Primo_Piano/Documents/2015/07_Luglio/White%20book.pdf

Henry Kenyon, “Navy views network infrastructure as a vital combat component”, in *DefenseSystems.com*, 9 June 2011, http://defensesystems.com/articles/2011/06/09/naval-it-day-greenert-network-as-combat-system.aspx

Maren Leed, *Offensive Cyber Capabilities at the Operational Level. The Way Ahead*, Washington, Center for Strategic and International Studies (CSIS), September 2013, http://csis.org/node/46679

Robert H. Legvold, “Managing the New Cold War”, in *Foreign Affairs*, Vol. 93, No. 4 (July/August 2014), p. 74-84, https://www.foreignaffairs.com/node/1113241

Edward N. Luttwak, *Strategy. The Logic of War and Peace*, Cambridge, Belknap Press, 2001

Stew Magnuson, “Top secret Air Force bomber program moves forward”, in *National Defense*, September 2014, http://www.nationaldefensemagazine.org/archive/2014/September/Pages/TopSecretAirForceBomberProgramMovesForward.aspx

Roberta Maldacea, Alessandro Marrone, Paola Sartori, *Defence Budgets and Industry: Tables and Graphs*, July 2015, http://www.iai.it/en/node/702

Carol Malouf e Ruth Sherlock, “ISIS Is Building Strength on Lebanon’s Doorstep”, in *BusinessInsider*, 20 January 2015, http://read.bi/15thyfi

Alessandro Marrone, “La non riforma della Difesa”, in *AffarInternazionali*, 24 February 2012, http://www.affarinternazionali.it/articolo.asp?ID=2544

Alessandro Marrone, “I quattro pilastri della riforma della Difesa”, in *AffarInternazionali*, 17 December 2012, http://www.affarinternazionali.it/articolo.asp?ID=2208

Scott Maucione, “DARPA wants white papers on ‘Squad X’ dismounted info-sharing”, in *InsideDefense.com*, 31 July 2014

Scott Maucione, “Multiple DoD components have high demand for spectrum innovation,” in *InsideDefense.com*, 31 December 2014, http://insidedefense.com/defensealert/multiple-dod-components-have-high-demand-spectrum-innovation.

Scott Maucione, “Pentagon eyes reforms in commercial SATCOM acquisition practices”, in *Inside the Pentagon*, 9 October 2014

Scott Maucione, “Upcoming DoD CIO cloud policy leaves questions over interoperability”, in *Inside the Pentagon*, 9 October 2014

Kevin McCaney, “Mobile satellite network gives Army swift artillery support”, in *DefenseSystems.com*, 2 December 2014, http://defensesystems.com/articles/2014/12/02/army-win-t-satellite-artillary-support.aspx

Paul McCleary, “US Army Presses Ahead on Manned-Unmanned Teaming”, in *Defense News*, 30 April 2013, http://www.defensenews.com/article/20130430/DEFREG02/304300018

Jordana Mishory, “DoD eyes interoperability in next-gen host-based cybersecurity strategy”, in *Inside the Pentagon*, 21 August 2014

Jordana Mishory, “DoD waives data link requirement so Navy can obtain eight systems”, in *Inside the Pentagon*, 14 August 2014

Jordana Mishory, “Official: DoD needs to better coordinate, oversee electronic warfare efforts”, in *InsideDefense.com*, 15 October 2014

Jordana Mishory, “Stratcom signs new space situational awareness data-sharing agreement”, in *Inside the Pentagon*, 4 September 2014

Ellen Mitchell, “Key Army official predicts growth of “Network Integration Evaluation” drills”, in *Inside the Army*, 3 October 2014

Ellen Mitchell, “Shyu: Army to procure $25M in technologies tested at NIE 14.1”, in *Inside the Army*, 8 September 2014

Pete Modigliani and Su Chang, *Defense Agile Acquisition Guide. Tailoring DoD IT Acquisition Program Structures and Processes to Rapidly Deliver Capabilities*, Mitre Corporation, March 2014, http://www.mitre.org/node/18951

Michele Nones and Marrone Alessandro (eds.), *The Transformation of the Armed Forces: The Forza NEC Program*, Rome, Nuova Cultura, October 2012 (IAI Research Papers No. 2), p. 31-38, http://www.iai.it/en/node/1387

Kris Osborn, "Marines fly helicopters with mini-tablet", in *DoD Buzz*, 5 April 2014, http://wp.me/pgSCu-8kt

Cheryl Pellerin, "Cybercom activates national mission force headquarters", in *DoD News*, 25 September 2013, http://www.defense.gov/news/newsarticle.aspx?id=120854

Walter Piatt, "The Future of European Collective Defense", in *CSIS Events*, 16 October 2014, http://csis.org/node/52206

Andrea Renda (ed.), *Global Outlook 2015: rapporto finale*, Rome, IAI, 29 April 2015, p. 92-100, http://www.iai.it/en/node/4141

Patrick A. Schrafft, "Enhancing fires with next-generation narrowband SATCOM", in Fires, July-August 2014, http://www.readperiodicals.com/201407/3410820761.html

Jason Sherman, "In event of sequester, entire modernization portfolio to be 'stretched out'", in *InsideDefense.com*, 14 October 2014

Sebastian Sprenger, "Army may break up major network program if results fall short", in *InsideDefense.com*, 14 October 2014

Sebastian Sprenger, "General Dynamics launches "Apollo" in bid to save its Army radio business", in *Inside the Army*, 3 October 2014

Brooks Tigner, "NATO urged to embed cyber defence into mission planning", in *Jane's Defence Weekly*, 23 September 2014

UK Government, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, 19 October 2010, https://www.gov.uk/government/publications/the-strategic-defence-and-security-review-securing-britain-in-an-age-of-uncertainty

UK Ministry of Defence Joint Forces Command and Philip Hammond, *New cyber reserve unit created*, 29 September 2013, https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit

UK Prime Minister's Office, *UK-France declaration on security and defence*, 17 February 2012, https://www.gov.uk/government/news/uk-france-declaration-on-security-and-defence

Alessandro Ungaro, Alessandro Marrone and Michele Nones, "Technological Innovation and Italian Armed Forces Training: Challenges and Opportunities", in *Documenti IAI*, No. 15|02e, January 2015, http://www.iai.it/en/node/3247

United Nations Peacekeeping, *Peace and Security*, http://www.un.org/en/peacekeeping/operations/peace.shtml

US Army Training and Doctrine Command (TRADOC), *The United States Army Operating Concept, 2016-2028*, TRADOC Pamphlet No. 525-3-1, 19 August 2010, https://fas.org/irp/doddir/army/opcon.pdf

US Army Combined Arms Center, *U.S. Army Mission Command Strategy, FY13-16*, June 2013, http://usacac.army.mil/cac2/Repository/Army_Mission_Command_Strategy_dtd_12June%202013.pdf

US Army Training and Doctrine Command (TRADOC), *The U.S. Army Operating Concept: Win in a Complex World, 2020-2040*, 31 October 2014, TRADOC Pamphlet No. 525-3-1, 31 October 2014, http://www.tradoc.army.mil/tpubs/pams/tp525-3-1.pdf

US Dept of the Army, *Army Equipment Program in Support of President's Budget 2015*, May 2014, http://www.army.mil/e2/c/downloads/348286.pdf

US Dept of Defence, *Instruction 2010.06, Materiel Interoperability and Standardization with Allies and Coalition Partners*, 29 July 2009, http://dtic.mil/whs/directives/corres/pdf/201006p.pdf

US Dept of Defence, *Instruction 8330.01, Interoperability of Information Technology (IT), including National Security Systems (NSS)*, 21 May 2014, http://dtic.mil/whs/directives/corres/pdf/833001p.pdf

US Dept of Defence, *Quadrennial Defense Review 2014*, March 2014, http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf

US Dept of Defence, *Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology*, March 2009, http://www.acq.osd.mil/dsb/reports/ADA498375.pdf

US Dept of Defence, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, January 2012, http://www.defense.gov/news/Defense_Strategic_Guidance.pdf

US Dept of Defence, Chairman of the Joint Chiefs of Staff, *Joint Publication 3-0: Joint Operations*, 11 August 2011, http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf

US Dept of Defence, Director Operational Test and Evaluation, *Army Programs, Network Integration Evaluation (NIE)*, 2011, http://www.dote.osd.mil/pub/reports/FY2011/pdf/army/2011nie.pdf

US Dept of Defence, Director Operational Test and Evaluation, *Reasons behind program delays: 2014 update*, 26 August 2014, http://www.dote.osd.mil/pub/presentations/ProgramDelaysBriefing2014_8Aug_Final-77u.pdf

US House of Representatives, Armed Service Committee, Subcommittee on Strategic Forces, *Statement of Gil I. Klinger*, 3 April 2014, http://docs.house.gov/meetings/AS/AS29/20140403/102037/HHRG-113-AS29-Wstate-KlingerG-20140403.pdf

US House of Representatives, Armed Service Committee, Subcommittee on Strategic Forces, *Statement of Douglas L. Loverro*, 3 April 2014, http://docs.house.gov/meetings/AS/AS29/20140403/102037/HHRG-113-AS29-Wstate-LoverroD-20140403.pdf

US Marine Corps, *Concepts and Programs: Aviation, Joint Strike Fighter (JSF)*, https://marinecorpsconceptsandprograms.com/programs/aviation/joint-strike-fighter-jsf

US Marine Corps, *Expeditionary Force 21. Forward and Ready: Now and in the Future*, 4 March 2014, http://www.mccdc.marines.mil/Portals/172/Docs/MCCDC/EF21/EF21_USMC_Capstone_Concept.pdf

US Marine Corps, *Service Campaign Plan for 2014-2022*, 21 May 2014, https://marinecorpsconceptsandprograms.com/sites/default/files/files/United%20States%20Marine%20Corps%20Service%20Campaign%20Plan%202014-2022.pdf

US Marine Corps, *USMC Concepts and Programs 2013*, http://www.hqmc.marines.mil/pandr/ConceptsandPrograms/ConceptsandPrograms2013.aspx

US Marine Corps Systems Command, *Modern Day Marine: Report to Industry*, 25 September 2014

US Senate, Committee on Armed Services, *Testimony of Frank Kendall*, 30 April 2014, http://www.armed-services.senate.gov/imo/media/doc/Kendall_04-30-14.pdf

US Senate, Committee on Armed Services, Subcommittee on AirLand, *Statement of Gen. John F. Campbell, Vice Chief of Staff, United States Army,* *on Fiscal Year 2015 Ground Force modernization and individual equipment modernization programs*, 9 April 2014, http://www.armed-services.senate.gov/imo/media/doc/Campbell-Barclay-Williamson_04-09-14.pdf

Stefan Wagstyl, "Germany plans early-warning defence against cyber attacks", in *Financial Times*, 10 November 2014, http://on.ft.com/1uXsbBS

Stephen Walt, "The Bad Old Days Are Back", in *Foreign Policy*, 2 May 2014, http://foreignpolicy.com/2014/05/02/the-bad-old-days-are-back

Marcus Weisgerber, "USAF General: DoD Must Change How it Buys Satellites", in *C4ISR & Networks*, 19 August 2014, http://www.c4isrnet.com/article/20140813/C4ISRNET06/308130001

IAI Research Papers

N. 1 *European Security and the Future of Transatlantic Relations*, edited by Riccardo Alcaro and Erik Jones, 2011

N. 2 *Democracy in the EU after the Lisbon Treaty*, edited by Raffaello Matarazzo, 2011

N. 3 *The Challenges of State Sustainability in the Mediterranean*, edited by Silvia Colombo and Nathalie Tocci, 2011

N. 4 *Re-thinking Western Policies in Light of the Arab Uprisings*, edited by Riccardo Alcaro and Miguel Haubrich-Seco, 2012

N. 5 *The transformation of the armed forces: the Forza NEC program*, edited by Michele Nones and Alessandro Marrone, 2012

N. 6 *Strengthening the Africa-EU Partnership on Peace and Security*, edited by Nicoletta Pirozzi, 2012

N. 7 *Stop Mass Atrocities*, edited by Luis Peral and Nicoletta Pirozzi, 2013

N. 8 *The Uneasy Balance*, edited by Riccardo Alcaro and Andrea Dessì, 2013

N. 9 *Global Turkey in Europe*, Edited by Senem Aydın-Düzgit, Anne Duncker, Daniela Huber, E. Fuat Keyman and Nathalie Tocci, 2013

N. 10 *Italy and Saudi Arabia confronting the challenges of the XXI century*, edited by Silvia Colombo, 2013

N. 11 *The Italian Civil Security System*, Federica Di Camillo, Alessandro Marrone, Stefano Silvestri, Paola Tessari, Alessandro R. Ungaro, 2014

N. 12 *Transatlantic Security from the Sahel to the Horn of Africa*, edited by Riccardo Alcaro and Nicoletta Pirozzi, 2014

N. 13 *Global Turkey in Europe II*, edited by Senem Aydın-Düzgit, Daniela Huber, Meltem Müftüler-Baç, E. Fuat Keyman, Jan Tasci and Nathalie Tocci, 2014

N. 14 *Bridging the Gulf: EU - GCC Relations at a Crossroads*, edited by Silvia Colombo, 2014

N. 15 *Imagining Europe*, edited by Nathalie Tocci, 2014

N. 16 *The Role of Italian Fighter Aircraft in Crisis Management Operations: Trends and Needs*, Vincenzo Camporini, Tommaso De Zan, Alessandro Marrone Michele Nones, Alessandro R. Ungaro, 2014

N. 17 I*n Search of a New Equilibrium. Economic Imbalances in the Eurozone*, Paolo Canofari, Piero Esposito, Marcello Messori, Carlo Milani, edited by Marcello Messori, 2015

N. 18 *West-Russia Relations in Light of the Ukraine Crisis*, edited by Riccardo Alcaro, 2015

N. 19 *Global Turkey in Europe III*, edited by Senem Aydın-Düzgit, Daniela Huber, Meltem Müftüler-Baç, E. Fuat Keyman, Michael Schwarz and Nathalie Tocci, 2015

N. 20 *The Role of Dual-Use Helicopters in the Security and Defence Field*, edited by Alessandro Marrone and Michele Nones, 2015

N. 21 *Promoting Stability and Development in Africa: How to Foster Cooperation between Public and Private Sectors*, edited by Marta Martinelli and Nicoletta Pirozzi 2015

N. 22 *Changing Migration Patterns in the Mediterranean*, edited by Lorenzo Kamel, 2015

N. 23 *Technological Innovation and Defence: The Forza NEC Program in the Euro-Atlantic Framework*, edited by A. Marrone, M. Nones and A.R. Ungaro, 2016

Printed in April 2016
with technology *print on demand*
at the press centre Nuova Cultura Rome
p.le Aldo Moro n. 5, 00185 Rome
www.nuovacultura.it

for orders: ordini@nuovacultura.it

[Int_9788868126513_17x24bn_LM02]