CAMPUS VIRTUALES

Recibido: 10-03-2019 / Revisado: 23-03-2019
Aceptado: 23-03-2019 / Publicado: 28-03-2019

Online distance learning as a factor of disruptive innovation in military education

La formación a distancia online como innovación disruptiva en la educación militar

Carlos González de Escalada Álvarez[1]

[1] Campus Internacional para la Seguridad y Defensa (CISDE), España

carlos@cisde.es

ABSTRACT. Defence and security education programmes ("DEFSEC") must adapt to new global threats and vulnerabilities to maintain effectiveness. Defence and security education of the future will require students to undertake highly specialised multi-discipline learning. This will afford schools and educational institutions an opportunity to introduce organic adaptations or even disruptive changes to achieve this goal. Online education is one of the clear vectors of this disruptive innovation, especially with regards to the cyberspace technology.
"DEFSEC" is the international acronym for Defence and Security. For the purposes of this work, DEFSEC entities are the Armed Forces, Security Forces and Intelligence Services.

RESUMEN. Los programas de formación de seguridad y defensa ("DEFSEC") están obligados a adaptarse a las nuevas amenazas y vulnerabilidades globales para seguir siendo eficaces. La educación en seguridad y defensa del futuro exigirá de los alumnos un aprendizaje multidisciplinar de alta especialización. Esto conlleva una oportunidad para que escuelas e instituciones educativas introduzcan adaptaciones orgánicas o incluso cambios disruptivos para lograrlo. La formación online es uno de los claros vectores de esa innovación disruptiva, máxime en el dominio del medio cibernético.
"DEFSEC" es el acrónimo internacional de Defensa y Seguridad. Para los propósitos de este trabajo, las entidades DEFSEC son las Fuerzas Armadas, Fuerzas de Seguridad y Servicios de Inteligencia.

KEYWORDS: Military education, Military training, e-learning, Distance learning, Online education, Disruptive innovation, Military academies, Cyberspace, Threats.

PALABRAS CLAVE: Educación militar, Formación militar, Aprendizaje online, Formación a distancia, Formación online, Innovación disruptiva, Academias militares, Ciberespacio, Amenazas.

1. Military training through history

Military training through history has adapted to the offensive and defensive needs of the military forces (Vidondo, 2006, p. 199). From ancient times to today, innovation has been a constant. This includes advances in which units operate in the war theatre, improvement in organisation or increase in military effectiveness (Voelz, 2016, p. 200).

Historically, strategists and generals have developed their tactical training and their weapons to win battles. Many of them were disruptive changes that upset military balance in favour of militaries that were ready to innovate. Today's top military world power, the United States, bases its effectiveness on the "technological superiority of its armed forces" (Doughert, 2018, p. 4). The first major disruptive change in the art of war was probably the Greek phalanx infantry formation, which dominated the art of Hellenic warfare for three centuries (Carey, 2006). The phalanx consisted of soldiers (hoplites) forming rectangular masses, armed with long spears and thus complicating the assault by other infantry or cavalry units. Over the centuries, disruptive innovations in land, sea and air combat have been constant. Clear examples are found in the complex formation of Roman legions, very disciplined even on the basis of corporal punishment (Kiesling, 2006); the binary disposition of the Inca battalion; the scientific revolution of the Navigation School of Sagres (Bermejo Díaz, 2014: 20); pikemen and arquebusier formations of the Spanish Tercio; the grouping of large formations of the Grand Napoleonic Army or the arrival of military academies, widespread today. In all these cases, military instruction and training has been at the service of the needs of their respective armies, which in turn served to counteract the surrounding threats.

From the technical point of view, innovations in weapons and systems have been constant. Some examples are: Some examples include:

- The closed infantry formation (Greek phalanx)
- The cataphract (armoured cavalry)
- Siege machinery
- The Longbow
- The Firearm
- The Airplane
- The Combat Vehicle
- The Submarine
- The Missile
- The Atomic Bomb
- Electronic warfare
- The Satellite
- The Internet

General Joe Allen (r) of the Marine Corps is now convinced that "artificial intelligence will change the balance of powers" (Allen & Husain, 2018) and he gives as an example the use of "Big Data" by China to control subversive movements; Two thousand years ago, the Germanic tribes were also convinced of the superiority of the Roman legions in land combat.

Each innovative army broke the balance of forces, at least momentarily, forcing the adversary to adapt in order to design and teach new tactics or weapons to recover the balance. Likewise, this historic and confirmed trend has accelerated exponentially in modern times. Since the beginning of the 20th century, the means in which it has been fought has grown.

The use of military aviation became widespread after World War I. Since the second half of the twentieth century, the launch of satellites and the threat of the cruise missile by the world powers have extended the offensive capacity of nations to the stratospheric and orbital space. Finally, in our historic present, the use of

information technologies and, particularly, the Internet, has broadened the battlefield to cyberspace.

In the last twenty years, there are many researchers who say that cyberspace needs to be added as a new battlefield, to those already existing: Nitzberg (1997), Solce (2008), Christian Czosseck and Kenneth Geers (2009), Philbin and Philbin (2013), to name a few.

The battlefield chronology can be summarised as follows:

- Land warfare (prehistory)
- Maritime warfare (ancient history)
- Air warfare (XX Century)
- Air warfare (XX Century)
- Cyber warfare (XXI Century)

A confrontation can occur using one of these means or several simultaneously.

2. The adaptation of military training through history

An examination of military history offers relevant lessons when interpreting security today. According to Sibul (2011, p. 94) an analysis using case studies helps in preparing future officers. According to Dr. Sibul, this method helps them cope with the present and future complexities of the operations.

Military training has always sought the greatest effectiveness of military forces in combat. The discipline and integrity of units under the stress of violent confrontation has been a constant concern. Another constant is that threats will continue to evolve, whether due to technological advances, social changes or the tireless ingenuity of the adversary.

Parker (2005, pp. 2-8) assures that the evolution of war in the west was initially based on the premise of technology and discipline. According to the same author, the art of war has evolved erratically, with periods of slow evolution, combined with brief periods of great technological leaps.

When a nation innovates, the military doctrine, armament and formation of the adversary will by necessity adapt, but at slower rate since it initially lacks the knowledge to do so, especially if it is a disruptive or revolutionary offensive system. The adaptation may be seen as necessary after an army has suffered a defeat, as happened when the Roman consul Publius Cornelius Scipio Africanus was defeated by the cataphracts (kataphraktoi), allies of the Carthaginian army (Sanz, 2014, p. 36). The use of battle vehicles in large formations demonstrated overwhelming effectiveness in the blitzkrieg, during the first European battles of World War II (Clark, 2016) in 1941. The acquisition of new revolutionary weapons systems, as was the invention of the atomic bomb, are still not available to the vast majority of nations (the power of destruction of these new systems have given rise to associated strategic concepts such as nuclear deterrence, mutual assured destruction or nuclear non-proliferation). In this sense, Sokolski (2004, p. V) claimed fifteen years ago that the thought of mutually assured destruction seemed to be in decline after the United States declared that destroying enemy neuralgic centres with nuclear force was not a legitimate endeavour. However, President Donald Trump's recent declarations of withdrawing from non-proliferation treaties has once again revitalised this dangerous concept of strategic thinking.

Another factor that affects military training is that there has been an unprecedented technological acceleration in the mere 100 years between the beginning of the 20th century and the 21st century. This has especially affected the military battlefield, which has culminated with the very doctrinal acceleration of the so-called Revolution of Military Affairs at the beginning of the 21st century (O'Hanlon, 2000, p. 25).

In addition to the emergence of three new warfare tactics in the last century (air, space and cyberspace),

communications technology makes the latter ubiquitous, allowing offensive attacks or the committing of crimes from anywhere in the world. In a US Senate committee in 2012, the then director of the FBI, Robert Mueller, explained that the cyber threat would probably be "the number one threat of the future" (Leithauser, 2012).

Danecki and Danecka (2004, p. 151) establishes a cause-effect relationship between pro-globalisation forces, anti-globalisation resistance and terrorism as an extreme form of reaction to the imposition of a globalising movement subject to interests. Patrick (2011, p. 3, p. 242) recalls that the global threats to the United States have ceased to be exclusively military, emanating also from poor and unstructured countries. Although the author refutes the "conventional wisdom" that being a weak state entails per se an inherent risk to international security, he does recognise that many threats come from failed states. In any case, society is globalised and threats are as well. Consequently, it is urgent to accelerate the adaptation of the military and police training institutions as first responders, to face them in a comprehensive manner.

3. Great challenges to international security

The most prominent emerging threats in the coming third decade of the 21st century, are:

1. Asymmetric and hybrid war conflicts. The democratic powers no longer declare war; they participate in contests, either unilaterally or in alliance with others. However, in some scenarios a new framework is drawn that is illustrated as the hybrid conflict: the emergence of nation-states in territorial armed confrontations (Crimea and Ukraine crisis).

2. Cyber-espionage, cyber-crime and cyber-attacks. The use of networks to carry out cyber espionage, cybercrime or cyber-sabotage missions is widely accredited. The most systematic of these conducted by nation-states is the advanced persistent threat. Cyber-aggressions cause very severe damage to the countries, companies, institutions or individuals attacked.

3. "Propaganda 2.0". Through social networks we are experiencing a new phenomenon, that of the organised use of disinformation, hoaxes, slander, fake news or tendentious misdirection. Some are leaked to agencies, media and social networks. These organised campaigns take on a strategic dimension when carried out by nation-states.

4. Global terrorism: Jihadist terrorism is a scourge that affects international security with massive attacks in many parts of the world.

5. Global organised crime: The borders of organised crime have been altered. Groups cooperate with each other and networks become denser thanks to the ease of communication.

6. Extremist, delegitimising, anti-system or subversive ideology: Ideologies contrary to the established order, which proliferate through populist or extremist movements, often delegitimise the legitimate use of force or the containment of frontiers before public opinion. This weakens the political strength of the ruling parties and makes weakens nations.

7. Energy dependence: The geopolitical positions of nations are limited by the greater or lesser dependence exercised by countries with energy surpluses.

8. Uncontrolled migratory movements. Today, both Europe and North America suffer the consequences of the massive influx of immigrants that politically destabilise nations. A disturbing consequence is that the increase in inhabitants reduces the intensity and quality of public services. The arrival of people without work permits triggers illegal recruitment and creates criminal pockets.

9. Systemic corruption Generalised corruption: Generalised corruption is a problem for nations that

carry out security policies of proven effectiveness. Corruption acts as a thinner for the adequate management of public resources.

10. Loss of inhibition of totalitarian countries because of the arms race: Countries that are less constrained by public opinion and the short-terms of political parties in office are better able to design multi-year weapons strategies. At this moment China is in a full arms race. Embarking on a similar military effort is something that would be politically inadmissible in Western nations.

The National Security Strategy[1], published by the Government of Spain in 2017, officially identifies fifteen threats, vulnerabilities and challenges. They are grouped as follows:

THREATS AND VULNERABILITIES
1. Armed conflicts
2. Terrorism
3. Organised crime
4. Proliferation of weapons of mass destruction
5. Espionage
6. Threats on critical infrastructures

GLOBAL THREATS AND VULNERABILITIES
7. Cyberspace
8. Maritime space
9. Airspace and Outer space

CHALLENGES
10. Economic and financial instability
11. Energy vulnerability
12. Irregular migration flows
13. Emergencies and catastrophes
14. Epidemics and pandemics
15. Climate change

Using these fifteen threats, vulnerabilities and challenges, hereinafter TVC's, as the official TVC's identified by the Government of the Kingdom of Spain, it is possible to draw some conclusions that will affect the degree of preparation of Spanish Defence and security institutions, and especially military training. Two tables (Table 1 and 2) have been produced that compare TVC's from a traditional and current concept of the use of Armed Forces (FFAA in Spanish), Security Forces and Corps (FFCCS in Spanish) and Intelligence Services (SI in Spanish). For example, thirty years ago military personnel would collaborate in flood relief as an extraordinary mission, but it was not direct competence as it is today since the creation of the Military Emergency Unit in 2006.

[1] 2017 National Security Strategy: a project shared by all and for all. Department of National Security. Presidency of the Government of Spain.

ESN 2017	Direct competence in the response or neutralisation: 1950 – 2000			
TVC. Threat, Vulnerability and Challenge	***Armed forces***	***Police and Security Forces***	***Intelligence***	***Non DEFSEC***
Armed conflicts	X		X	
Terrorism (national)		X	X	
Organised crime		X		
Proliferation of weapons of mass destruction			X	
Espionage			X	
Critical infrastructures				X
Cyberspace				X
Maritime space	X	X		
Airspace and Outer Space	X			
Economic and financial instability				X
Energy vulnerability				X
Irregular migration flows		X		
Emergencies and catastrophes				X
Epidemics and pandemics				X
Climate change				X
	20%	**26,6%**	**26,6%**	**46,6%**
				Source: In-house.

Table 1. ESN 2017. Direct competence in the response or neutralisation: 1950 – 2000. Source: In-house.

The examination of the fifteen TVC's draws a first conclusion: from a traditional concept, only 20% of TVC's are military in nature: armed conflicts, maritime space and airspace and outer space. From the same concept, only 26.6% of them would be the direct competence of the Security Forces (State, autonomous community and local). From this concept, there is no great convergence of action between the Armed Forces, the FFCCS and the SI, with little in the area of terrorism (FFCCS and SI) and in the protection of maritime space (FFAA and FFCCS). Also, up to 26.6% of TVC's, more than a quarter, are traditionally not considered part of the military, police or intelligence: economic instability, energy and financial vulnerability, epidemics and pandemics and climate change. These TVC's today represent a novelty, precisely for the competent institutions of their neutralisation to guarantee national security.

ESN 2017	Direct competence in the response or neutralisation: 2000 – 2020			
TVC. Threat, Vulnerability and Challenge	***Armed forces***	***Police and Security***	***Intelligence***	***Non DEFSEC***
Armed conflicts	X		X	
Terrorism (international)	X	X	X	
Organised crime		X	X	
Proliferation of weapons of mass destruction			X	
Espionage	X		X	
Critical infrastructures	X	X	X	X
Cyberspace	X	X	X	X
Maritime space	X	X		
Airspace and Outer Space	X			
Economic and financial instability			X	X
Energy vulnerability			X	X
Irregular migration flows		X	X	X
Emergencies and catastrophes	X			X
Epidemics and pandemics				X
Climate change				X
	53,3%	**40%**	**66,6%**	**53,3%**
				Source: In-house.

Table 2. ESN 2017. Direct competence in the response or neutralisation: 2000 – 2020. Source: In-house.

From a current concept of employment of defence and security institutions (FFAA, FFCCS and SI), or DEFSEC entities, the allocation of duties varies significantly. There is a current security policy in Spain that advocates a greater collaborative convergence of defence and security entities in the interest of comprehensive security (González de Escalada, 2018, pp. 235-250). This entails that the Armed Forces, through the Army,

Navy, Air Force and Common Agencies, have direct jurisdiction over eight TVC's: armed conflicts, terrorism[2], espionage, critical infrastructures, cyberspace, maritime space and emergencies and catastrophes. In this way, they go from having direct competence in 53.3 of the TVC's, a very significant increase from 20% of a traditional concept of the use of force.

Hence, the FFCCS are now competent to act against six TVC's: terrorism, organised crime, critical infrastructures, cyberspace, maritime space and irregular migratory flows, 40% against the previous 26.6%. The intelligence services also suffer a notable competency increase, from 26.6% to 66.6%.

In addition, the TVC's in which the performance of several of our defence and security entities converge are also extended to cyberspace and critical infrastructures (now the competence of both DEFSEC, and non-DEFSEC entities). To a lesser extent, terrorism and irregular migratory flows are also.

4. Emergence of cyber warfare and the increase of TVC's

The DEFSEC entities face a simultaneous double challenge: the emergence of cyber warfare as a new theatre of operations and the increase of TVC's they must now face. Currently, the Armed Forces have to fight against 170% more TVC's than a few decades ago. This adds new components that do not have to be part of the doctrinal heritage of the Armed Forces.

The modern threat has unprecedented components, some of which are totally global. Many TVC's are heterogeneous in that they contain imbricated components of an organisational, political, criminal, ideological, sociological, economic or technological nature. That is, a terrorist group may re-enact criminal acts to finance itself, or a subversive movement resorting to propaganda 2.0 to gain notoriety.

Threats also mutate. Political destabilisation through the targeted use of social networks is a very recent phenomenon. As the battlefield expands to the cyberspace, nations have had little time to prepare for the changes taking place in the technology sector. This adaptation is not easy given that cyber-strategists are scarce.

Paradoxically, the expansion of threats and the battlefield compromises the effectiveness of weapons systems for conventional combat, including those of technological superiority. If the manipulation of the American public opinion instigates opposition to a military intervention, its war potential is de facto neutralised. Creating a group of cyber-activists and political cyber-stalkers is cheaper than mobilising the V I Fleet, but the former is capable of mooring the latter.

5. Challenges for a new educational paradigm in military training

The Spanish Armed Forces were prepared and trained for conventional combat. Currently, the military requires new skills in cyber security, cyber defence, cyber espionage, the defence of critical infrastructures, combat against jihadist terrorism an intervention in natural disasters. Without discarding, in the near future, direct competencies in the containment of migratory flows, as in Italy. All of these are new areas that are not part of the traditional training in military study centres.

The emergence of new TVC's entails a logical need to adapt in order to face them. As Domínguez León explains (2018, p. 135): "updating appropriate methodologies means improving the foundations in order to guide security through police prevention." The promotion of newly minted defence and security competencies will prevent future damage.

In Spain, the threat of jihadist terrorism is very clear, the result of radicalisation processes that assume an extreme ideology (González, 2015, p. 5). Although its mitigation is clearly a police responsibility, its origin may be in foreign combatant groups such as Daesh or Al-Qaida, which have required the intervention of Spanish

[2] The Antiterrorist Alert Level of the Ministry of Interior, in level-5, entails the use of military units for citizen protection.

forces in different multinational missions. There are also confluences between cyber warfare and the rest of the TVC's, which multiply the harmful power of each threat. Especially worrisome is the binomial of new technologies - jihadist terrorism, used even through children's video games (Carmona, 2016, pp. 66-67). For military training, this represents the need to incorporate complex competencies in an environment in which technical trainers are scarce. As explained by Pérez and Guirao (2017, p. 75) "defence capabilities are inevitably compromised by the dynamism of cyberspace", which in turn increases the challenge of finding trainers who are up to date with the latest cyber threats.

Complex is also the approach to illegal immigration, a problem that is worsening in Spain and that requires a holistic vision of the European Union's comprehensive focus towards the sources (De Carlos Izquierdo, 2018, p. 14), which currently escapes the control of the Armed Forces.

The control of cyber warfare, the fight against terrorism by parastatal groups, the protection of critical infrastructures and the possible action against massive migratory flows, will necessarily entail an enrichment of the military doctrine in hitherto unknown areas.

Among the adaptation needs of developed nations include the following:

1. Integrated defence policies, including national security multi-threat strategies.
2. Creation of national multidisciplinary Security Councils, including the participation of the private sector and academic institutions.
3. Greater coordination and integration between armed forces, internal security forces and intelligence services.
4. Development of larger and more coordinated cyber security and cyber defence of public structures.
5. Greater budget allocation in defence and security.

The emergence of disruptive threats entails a slow adaptation for countries that are in the "caboose". Whenever a competency is acquired to do something new, the first step will be to learn how to do it, second teach how to do it and finally, to do it. Learning will always be the first step, training the second step and competent acting the third.

This approach puts universities, academies, schools, centres or institutions related to defence and security training, including the military, at the forefront. These organisations will be the protagonists in neutralising the many threats of tomorrow. The most important challenges faced are:

6. National structures engineered for conventional military conflict and internal security.
7. Chronic deficit in defence spending in Western countries.
8. Inadequate development of multi-threat doctrines in many countries, which hinders cooperation.
9. Shortage of expert professors and researchers in geo-security, defence policy or cyber security (compared to other scientific disciplines).

6. Opportunities for organic adaptation of military training

Every uncertain panorama entails a series of opportunities to react and lead. Perhaps the first step is to understand the problem before trying to solve it. The dilemma arises from facing the increase of TVC's with limited resources and time. TVC's whose neutralisation require planning the incorporation of new skills and abilities in the Force, to the detriment of others. In this sense, governments have the possibility of adapting to the new reality (organic adaptation) or to revolutionary innovate (disruptive leadership), which also affects military training institutions.

Among the opportunities for organic adaptation, the following is proposed:

10. Adaptation of the military curriculum.
11. Increase of the training related to cyberspace.
12. Increase in research through specialised publications.
13. Training of expert technologists in defence and security in the military and police and intelligence services (cyber-intelligence).
14. Incorporation of civilian trainers.

The broadening of the minimum competences that military (and police) must possess will entail a transformation of the training programme to cover new needs. There is a growing range of training in universities and graduate institutes, which complements the activity of public schools. Having properly trained personnel is the first step to undertake whatever national security policy that needs to be implemented.

7. Opportunities for disruptive leadership in military training

One of the most important elements to generate disruptive advances in military training of the future will be the intensive use of interactive online media in military training. Online distance learning has been a before and after in the global academic scene, which has also affected defence (González de Escalada, 2016, p. 9). Culkin (2017) affirms that the current North American military doctrine allows the establishment of evaluation designs which combine the flexibility of interactive models, the conceptual planning of design methodology and the rigor of the frames that are placed in the theoretical context of distance learning.

A study by Tung, Huang, Keh and Wai (2009, pp. 653-666) demonstrated the feasibility of distance learning for a group of senior Taiwanese officers (colonel or equivalent); specifically in Advanced Military Education programmes[3] in joint operations. The results were satisfactory, although the authors insist that planning should be done carefully. Tung et al. (2009, p. 655) also report that a study by Russell (1997) analysed 355 teaching programmes, including those by post, face-to-face and online, conducted by students at all levels of academic achievement. After compiling the results of numerous studies, he concluded that 90% of these showed that, in terms of student performance, there were no significant differences between distance learning and face-to-face training.

The process of competency adaptation must have cyber warfare as its main objective, whose technological power has a direct effect in most of the TVC's. There are very few professional spheres outside the technological environment.

The intensive use of online training can revolutionise the scope of military training, when precisely the digital nature of training is especially suitable for training aimed at achieving a military superiority over cyber warfare. Achieving the ubiquity of online training and the implementation of programmes designed to achieve superiority in cyberspace is an opportunity for a dual disruption for nations that clearly understand its benefits. Achieving military superiority in conventional weapons systems is only within reach of the major powers. On the contrary, achieving superiority in cyber warfare will be feasible also for medium powers.

By taking disruption to its ultimate consequences, it would be possible to conceive, plan, establish and train a specific army specialised in the cyber warfare. A new military branch, of equal importance as the Army, Navy and Air Force, and commanded by a four-star general[4]. This Cyber Defence Army would specialise in obtaining strategic, operational and tactical superiority in cyber combat and cyber-intelligence operations. If each battlefield requires specialised forces, this step would seem logical and possibly the most revolutionary step undertaken by the armed forces of any country.

In any case, the disruptive domain of the cyber battlefield would be favoured by the following measures of

[3] Advanced Military Training.

[4] This would correspond to an army general in Spain.

academies or military schools:

1. Opening of military academies to civilian personnel as a means of interaction and recruitment.
2. Assimilation of military academies with a national defence university.
3. Recruitment and integration of postgraduate graduates specialising in technology, networks and social networks.
4. Recruitment, direction and support of ethical "hacker" groups to train trainers.
5. Creation of exclusive military academies for online education, with the following advantages:
   - Elimination of physical barriers.
   - Elimination of temporary barriers.
   - Sensible reduction of cost / student.
   - Opportunity to offer continuous training and higher qualifications.
   - Opportunities to offer undergraduate and doctorate degrees.
   - Specialisation in threats 2.0.
6. Creation of technology-based reserve corps (Reserves 2.0).
7. Creation of fundamental cyberspace specialties.
8. Support of academic agreements between armed forces, universities and specialised institutes, for the exchange of students and professors.
9. Person policies with detection systems for recruiting military and police personnel with high capacities or gifted, for cyber security, cyber defence and cyber-intelligence.
10. Recruitment systems of civilian specialists identified as having military values.

8. Prospective advancement of military training

Training in defence and security of the future will adapt, sooner or later, to the nature of the threats that society wants to fight. Although a threat is not the same as the perception of a threat, there are new risks that are becoming very clear. In a prospective exercise, we can see what the military training of the future will look like:

- The number of military units specialised in cyber warfare will increase.
- The technological and cyber-logical training component will increase so as to improve the capabilities of the cyber security and cyber defence systems.
- It will teach an integrated concept of defence and security so as to neutralise growing and changing threats.
- Online training will proliferate with the consequent dilution of time-space and cost reduction barriers.
- The comprehensive security concept will become consolidated with the consequent narrowing of the collaboration between armed forces, internal security forces, intelligence services and civil entities.
- Collaboration with public and private educational institutions will be encouraged.
- The joint doctrine will broaden to include the cybernetic component.
- The combined cybernetic component doctrine will move forward.

9. Conclusions

Threats are ever changing and are currently proliferating and mutating faster. The rise of new technologies creates a new theatre of cyber operations, a new battlefield, in addition to those already known: land, sea, air and space. Operations in cyberspace do not rest and can take place from anywhere in the world. 24 hours a day, 365 days a year, there are people, bands or organised groups that spy, sabotage, commit crimes or defame through an ethereal, unfading digital media.

Other phenomena such as globalised terrorism, the need to protect critical infrastructures, migratory flows, delegitimising populist movements, climate change, energy dependence or economic instability represent new threats to which DEFSEC entities will have to adapt through training and organic evolution. This will have a direct impact on military training, which will be forced to change.

There is an opportunity to implement defence and security policies focused on achieving technological leadership at a comparative cost lower than modern conventional land, naval or aerial weapons systems.

Academies and military and police schools are already at the forefront to lead the doctrinal reformulation before a new realm of national and international threats. Military training has the objective opportunity to progressively implement online education programmes, especially in a society used to communicate through mobile and computer applications on a daily basis. The promotion of interactive education supposes a disruptive element within the reach of military academies and schools. There is also the opportunity to promote a dual disruptive change if, in the scope of interactive military training, the goal of obtaining superiority in the cyber battlefield stands out.

The creation and training of a hypothetical Cyber Defence Army equal in rank as its Land, Naval and Air counterparts, offers a new field of exploration that would revolutionise the Spanish military doctrine, including military training.

Cómo citar este artículo / How to cite this paper

González de Escalada Álvarez, C. (2019). Online distance learning as a factor of disruptive innovation in military education. *Campus Virtuales,* 8(1), 87-98. (www.revistacampusvirtuales.es)

References

Allen, J.; Husain, A. (2018). Ai Will Change the Balance of Power. U.S. Naval Institute Proceedings, 144(8), 26-31.
Bermejo Díaz, A. C. (2014). Navegación marítima, estudios de náutica y experiencias bajo las estrellas. Universidad de la Laguna.
Carey, B. T. (2006). The phalanx dominated Greek warfare for three centuries, but fell before combined-arms forces. Military History, 23(6), 69-72.
Carmona, M. E. E. (2016). Las redes sociales y los videojuegos como mecanismos de captación del Daesh. Revista de Pensamiento Estratégico y Seguridad CISDE, 1(2), 65-76.
Czosseck, C.; Kenneth, G. (2009). The Virtual Battlefield: Perspectives on Cyber Warfare (Vol. 3). Ios Press.
Clark, L. (2016). Blitzkrieg: Myth, Reality, and Hitler's Lightning War: France 1940. Gran Bretaña: Atlantic Books.
Culkin, D. T. (2017). Military design insights for online education program evaluation: A revised theoretical construct. American Journal of Distance Education, 31(4), 258-274.
Danecki, J.; Danecka, M. (2004). At the Roots of Global Threats: Development Dilemmas. Dialogue & Universalism, 14(10-12), 149-152.
De Carlos Izquierdo, J. (2018). Presente y futuro de la Unión Europea. La crisis migratoria. Revista de Pensamiento Estratégico y Seguridad CISDE, 3(1), 9-16.
Domínguez León, J. (2018). Pensamiento estratégico, prospectiva, violencia extrema y terrorismo emergente: tareas inmediatas. Problemas emergentes en seguridad: retos y amenazas presentes y futuros (pp. 135-176). Sevilla: CISDE Editorial.
Doughert, G. M. (2018). Promoting disruptive military innovation: Best Practices for DoD experimentation and prototyping programs. Defense Acquisition Research Journal: A Publication of the Defense Acquisition University, 25(1), 2-29.
González de Escalada, C. (2016). Lecciones aprendidas sobre formación interactiva en seguridad y defensa: El caso de CISDE. Revista de Pensamiento Estratégico y Seguridad CISDE, 1(1), 8-16.
González de Escalada, C. (2018). Del concepto de Defensa al de seguridad integral. Problemas emergentes en seguridad: retos y amenazas presentes y futuros (pp. 235-250). Sevilla: CISDE Editorial.
González, J. A. M. (2015). La política de defensa de España ante la amenaza del terrorismo yihadista. RESI: Revista de estudios en seguridad internacional, 1(1), 1-16.
Hanley, B. (2007). The West & the Rest: Globalization and the Terrorist Threat. War, Literature & the Arts: An International Journal of the Humanities, 19(1/2), 368-371.
Hustad, K. (2014). Next generation of cyber defenders prepare for expanding battlefield. Christian Science Monitor, April 29.
Kiesling, E. C. (2006). Corporal Punishment in the Greek Phalanx and the Roman Legion: Modern Images and Ancient Realities. Historical Reflections/ Réflexions Historiques (pp. 225-246).
Leithauser, T. (2012). Cyber threat is spy agencies' top worry after terrorism, nukes, senators told. Cybersecurity Policy Report, 1.
Nitzberg, S. (1997). The cyber battlefield-is this the setting for the ultimate World War?. In Technology and Society (1997), Technology and Society at a Time of Sweeping Change. Proceedings 1997 International Symposium on (pp. 100-106). IEEE.
O'Hanlon, M. (2000). Technological change and the future of warfare. Washington DC: Brookings Institution Press.

Patrick, S. (2011). Weak links : fragile states, global threats, and international security. Oxford, New York: Oxford University Press.
Patrick, S. (2006). Weak states and global threats: Fact or fiction?. Washington Quarterly, 29(2), 27-53.
Parker, G. (Ed.). (2005). The Cambridge history of warfare. Cambridge University Press.
Pérez, J. A.; Guirao, I. D. J. A. (2017). Cyberspace and European security. Revista de Pensamiento Estratégico y Seguridad CISDE, 2(2), 71-78.
Philbin, G.; Philbin, T. R. (2013). Finding the New High Ground in Cyber War: Malware as an Instrument of War. Journal of Homeland Security & Emergency Management, 10(1), 1-8.
Russell, T. L. (1997). The "No significant difference" phenomenon as reported in 248 research reports, summaries, and papers. North Carolina State University.
Sanz, A. S. (2014). Después de Alejandro el Grande, el desarrollo de las tácticas bélicas griegas en el imperio seléucida. Revista Electronica de Antiguidade, Universidad do Estado do Rio de Janeiro, VII(1), 23-51.
Sibul, E. A. (2011). Military History, Social Sciences, and Professional Military Education. Baltic Security & Defence Review, 13(1), 71-99.
Sokolski, H. D. (2004). Getting MAD: nuclear mutual assured destruction, its origins and practice. DIANE Publishing.
Solce, N. (2008). The battlefield of cyberspace: The inevitable new military branch-the cyber force. Alb. LJ Sci. & Tech., 18, 293.
Tung, M. C.; Huang, J. Y.; Keh, H. C.; Wai, S. S. (2009). Distance learning in advanced military education: Analysis of joint operations course in the Taiwan military. Computers & Education, 53(3), 653-666.
Vidondo, J. M. R. (2006). La enseñanza militar en el alto mando: historia, organización y metodología. Educación XX1, 9(1).
Voelz, G. (2016). Catalysts of Military Innovation: A Case Study of Defense BIOMETRICS. Defense Acquisition Research Journal: A Publication of the Defense Acquisition University, 23(2), 176-201.