RUSSIA'S HYBRID WAR AND ITS IMPLICATIONS FOR DEFENCE AND SECURITY IN THE UNITED KINGDOM

Sascha-Dominik Dov Bachmann[1]
University of Bournemouth
Anthony Paphiti[2]

Abstract

This article uses the example of Russia's aggressive action against Ukraine as an example of a new form of contemporary war fighting, namely hybrid war, and discusses how Russia has been successful in exploiting vulnerabilities of its opponents. The article reports on the United Kingdom as a case study to discuss potential threats and how these can be countered. While using the United Kingdom as an example, the ramifications of such a hybrid approach also apply to South Africa as a state which is vulnerable in respect to economic warfare, cyberattacks and its energy sector. The suggested counteractions could also be seen as lessons learned for a future South African scenario**.** It is a further development of a short submission to the Defence Select Committee of the UK House of Commons.

Introduction

Russia's illegal annexation of Crimea in 2014 and its open support of the separatists in the bloody conflict taking place in Eastern Ukraine since 2015 together with the global war against ISIL/Daesh in Iraq and Syria have brought a new terminus of conflict terminology into the dictionary: the term of Hybrid War.[3]

This article introduces the concept of hybrid warfare and discusses the vulnerabilities arising from the threat of Russia's potential use of such a mode of war fighting against the United Kingdom their legal context. In addition, the findings of this short contribution will also aid in assessing similar threats posed by non-state actors such as ISIL/Daesh and with regard to evolving new threat scenarios such as

Scientia Militaria, South African Journal of Military Studies, Vol 44, No. 2, 2016, pp. 28–67.
doi : 10.5787/44-2-1175

China's increasingly menacing stance in the South Sea with its ramifications for Association of Southeast Asian Nations (ASEAN) members.

The wealth of opportunity that hybrid warfare offers is extensive and, used well, can provide states with the means to do enormous damage, militarily and/or commercially, with little risk of attribution, particularly in the realm of cyber activity, and with minimum cost in terms of manpower and equipment. The effect can be devastating and can undermine vital institutions of the state. In addition, they stand a good chance of getting away with it. The general rapporteur to the North Atlantic Treaty Organization (NATO) has already pointed out:

> Hybrid warfare exploits domestic weaknesses via non-military means (such as political, informational, and economic intimidation and manipulation), but is backed by the threat of conventional military means. While the concept of hybrid warfare is not new, its application by Russia, and to a lesser extent by Daesh, against NATO member states' interests present new challenges to the Alliance.[4]

For these reasons, states must be prepared to face these new and varied threats in order to protect themselves, their citizens and their infrastructure from attack. Some of the main types of hybrid threat are set out in the section on forms of hybrid warfare. Only by recognising that these threats exist and that are easily implemented can the United Kingdom go on to examine how it needs to identify any specific threat, assess its potential damage if not countered, and then determine the measures it takes to neutralise it – or turn it to its own advantage, once the issue of attribution has been determined. Which threshold a hybrid attack must reach before it is considered an armed attack is considered below, in the section on the challenges to the United Kingdom. Any hybrid attack on a NATO member state, which reaches the threshold of an armed attack, would engage the mutual defence obligations under the NATO Treaty. The stakes are, therefore, very high.

Russian doctrinal thinking has been keenly influenced by what has come known as "the Gerasimov Doctrine",[5] which first appeared in the *Military-Industrial Kurier*, on February 27, 2013. General Gerasimov wrote,

> In the 21st century we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template.

Hybrid war

'Hybrid war' as a mode of war-fighting is not new and has its origins in the concept of 'hybrid threats', which was coined in the United States (US) military-specific literature as a result of the review of the military conflict between Israel and Iran-supported Hezbollah during the second Lebanon war of 2006. Hybrid threats in the context of asymmetric conflicts mostly consist of a blend of unconventional and conventional means of warfare, their tactics and methodology.[6]

Hybrid threats outside the context of conventional military conflict can be influenced by a variety of factors, which are deliberately provoked by different actors, and can be exploited. Hybrid threats are the result of a new enemy (state and non-state actors) and a new action spectrum. Such threats pose new challenges to policy and rule of law.

As early as 2010, NATO recognised hybrid threats were a new security risk and designed a new NATO Bi-Strategic Command Capstone Concept, describing hybrid threats as threats emanating from an adversary who combines both conventional and unconventional military methods to achieve its goals. Hybrid threats refer to "those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives". [7]

In the following two years, NATO drew up a specific threat catalogue, which identifies security-specific risks beyond conventional warfare threats: nuclear proliferation, terrorism, cybercrime and cyberwar, organised crime and its role in drugs, arms and human trafficking, migration, ethnic and religious conflicts, population conflicts due to resource scarcity and globalisation.

NATO recognised that such threats may amount to a concrete threat to the alliance or that NATO could be authorised by the United Nations, because of their capacity, to intervene. Recognising this, NATO worked on a related global approach (comprehensive approach) in order to counter these risks. This approach envisaged involving state and non-state actors in a comprehensive defence strategy that combines political, diplomatic, economic, military technical and scientific initiatives. Despite intensive work on this approach as part of a 'countering hybrid threats' experiment in 2011, the NATO project work in 2012 had to stop due to a lack of support from their members.

Given the Russian aggression in Ukraine since 2014, the question arises whether the cancelling of this project was not premature. Since 2014, NATO has resumed its work on the hybrid warfare project with the aim of determining

whether this form of warfare requires a redefinition of Western military doctrine (as a new category in full spectrum operations). Whether the application of hybrid warfare by Russia will result in a return of the Cold War against the background of Russia's Eastern European hegemonic ambitions, remains to be seen.[8] What has become clear, however, is that "hybrid warfare 'has the potential to transform the strategic calculations of potential belligerents [it has become] increasingly sophisticated and deadly'".[9]

Forms of hybrid warfare

A hybrid attack may take many forms, and based on available sources, the following have been identified as relevant for a developed country such as the United Kingdom. The most obvious threat is of cyberattacks on military command and control, air traffic control systems, hospital power supplies, the electricity grid, water supplies, nuclear power, satellite communications, Internet attacks on the banking system, and cyberattacks on dams/water supply and other eco threats.

One of the oldest forms of hybrid threat is that of espionage and surveillance, the purpose of which is to obtain military or commercial secrets. The use of spies to infiltrate government and key organisations has the potential to provide very valuable information. However, if that espionage is discovered, the target state could play the double game and feed disinformation back to the targeting state. By way of example, in January 1976, the Concorde, a new supersonic aircraft made its maiden flight. It was the product of Anglo–French engineering. It shared the skies with a remarkably similar-looking aircraft, the Tupolev TU-144, nicknamed 'Konkordski'. There was a theory that the Anglo–French Concorde team knew that the then Soviet Union intended to steal their plans, so they circulated a set of dummy blueprints with deliberate design flaws. The consequence for Konkordski was a rather tragic ending at the Paris air show in June 1973, when it "went into an abrupt dive, began to break up and crashed into a fireball that consumed a neighborhood in the village of Goussainville".[10]

The use of propaganda/misinformation/PsyOps using the information sphere could also be a most effective means of hybrid warfare. This is highlighted in several contexts below.

One aspect which is perhaps not given the attention it should is that of foreign investors gaining a controlling interest in essential services, such as energy supplies, water supplies, airports and sea ports. This is discussed in the section on vulnerability and dependency of essential services, key infrastructure and utilities.

The use of populations and migration is discussed below in the section on mass migration and hybrid war. This is an aspect, which touches sensitive nerves and has been exploited for political as well as military advantage.

Other forms of hybrid warfare are state-to-state aggression behind the mantle of a 'humanitarian intervention', and terrorism.

On the military front, use of special forces – 'little green men' – is another form of hybrid warfare, demonstrated effectively in Crimea/Donetsk (Ukraine) and the denial of their existence by Russia.

The study on which this article reports, examined some of these hybrid methods in more detail and this article highlights relevant legal points where appropriate.

Russia's use of hybrid warfare

In a Keynote speech at the opening of the NATO Transformation Seminar on 25 March 2015, NATO Secretary General Jens Stoltenberg remarked:[11]

> Russia has used proxy soldiers, unmarked Special Forces, intimidation and propaganda, all to lay a thick fog of confusion; to obscure its true purpose in Ukraine; and to attempt deniability. So NATO must be ready to deal with every aspect of this new reality from wherever it comes. And that means we must look closely at how we prepare for; deter; and if necessary defend against hybrid warfare.
>
> To be prepared, we must be able to see and analyse correctly what is happening; to see the patterns behind events which appear isolated and random; and quickly identify who is behind and why.
>
> So therefore, we need to sharpen our early warning and improve our situation awareness. This is about intelligence, expert knowledge and analytical capacity. So we know when an attack is an attack.

The employment of hybrid methods has been evident from Russia's activities in Crimea and the Donbas region of Ukraine, with its deployment of 'little green men', namely soldiers wearing unmarked uniforms that make direct state attribution difficult. According to Mark Galeotti,

> The conflict in Ukraine has demonstrated that Moscow, in a bid to square its regional ambitions with its sharply limited resources, has assiduously and effectively developed a new style of 'guerrilla geopolitics' which

> leverages its capacity for misdirection, bluff, intelligence operations, and targeted violence to maximise its opportunities. However, it is too soon to declare that this represents some transformative novelty, because Moscow's Ukrainian adventures have not only demonstrated the power of such 'hybrid' or 'non-linear' ways of warfare, but also their distinct limitations.[12]

While there may be limitations to the way in which these methods were used in Ukraine, the use of unattributable military personnel provides expert assistance to an enemy and, even if not directly engaged in hostile acts, provides advice and assistance to those who carry out such acts. Nevertheless, the seriousness of the threat posed by such forces should not be under-estimated. General Breedlove, a former Commander, US European Command (EUCOM) and the former Supreme Allied Commander Europe (SACEUR), has been reported as saying, "if Russia does what it did in Crimea to a NATO state, it would be considered an act of war against the alliance".[13]

In his view –

> The most important thing is that NATO nations are prepared for the so-called green men: armed military without insignia who create unrest, occupy government buildings, incite the population; separatists who educate and give military advice and contribute to the significant destabilisation of a country … there is a danger that this could also happen in other eastern European countries.

In Russia's 2010 Military Doctrine, modern warfare is described as entailing "the integrated utilization of military force and forces and resources of a non-military character," and, "the prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favorable response from the world community to the utilization of military force".[14]

Andrew Monaghan has remarked, "while the term hybrid war offers some assistance to understanding specific elements of Russian activity, it underplays important aspects discussed by Gerasimov, and offers only a partial view of evolving Russian activity, capabilities, and intentions".[15]

Monaghan believes –

> [T]his supposedly new form of war conferred numerous advantages on Moscow, observers argued, since it heightened the sense of ambiguity in Russian actions, and provided Russian leadership with an asymmetric tool

> to undercut Western advantages: since Moscow would be unable to win a conventional war with the West, it seeks to challenge it in other ways. Furthermore, it fits readily into Western debates about the increasing roles of special forces and strategic communications in conflict.

Galeotti points out that[16] Russia has invested disproportionate resources into the assets most useful for such conflicts, to "reflect how this is a way of war which even more explicitly than most targets not the opponent's military or even economic capacity, but their will and ability to fight at all".

In Ukraine, Russia employed a hybrid strategy by combining irregular warfare (the 'little green men') and cyber-warfare to achieve its strategic objectives. Reuben F Johnson, writing in *IHS Jane's Defence Weekly*, on 26 February 2015, considered that "Russia's hybrid war in Ukraine 'is working'." Russia had combined a substantial ground force of 14 400 Russian troops supported by tanks and armoured fighting vehicles, backing up the 29 300 illegally armed formations of separatists in eastern Ukraine. In addition, they used electronic warfare (EW) and

> what appear to be high-power microwave (HPM) systems to jam not only the communications and reconnaissance assets of the Ukrainian armed forces but to also disable the surveillance unmanned aerial vehicles (UAVs) operated by ceasefire monitoring teams from the Organisation for Security and Co-operation in Europe (OSCE). Russian EW teams have targeted the Schiebel Camcopter UAVs operated by the monitors and 'melted the onboard electronics so that drones just fly around uncontrolled in circles before they crash to the ground'.
>
> Russian EW, communications and other units central to their military operations are typically placed adjacent to kindergartens, hospitals or apartment buildings so that Ukrainian units are unable to launch any strikes against them without causing unacceptable and horrific collateral casualties.[17]

These EW activities probably amount to the use of force constituting an armed attack by Russia, thereby rendering such EW equipment liable to legitimate attack. As such, an international armed conflict would exist. Consequently, positioning such assets close to civilians and civilian objects is a breach of the laws of armed conflict, in particular Articles 51(7) and 58 of Additional Protocol I (AP I),[18] which prohibit the presence or movements of the civilian population or individual civilians in order to render certain points or areas immune from military operations (use of human shields),

> [I]n particular in attempts to shield military objectives from attacks or to shield, favour or impede military operations. The Parties to the conflict shall not direct the movement of the civilian population or individual civilians in order to attempt to shield military objectives from attacks or to shield military operations.

The commentary to Article 58 points out that this extends to the need for care in particular during the conflict to avoid placing troops, equipment or transports in densely populated areas.

Art. 58 AP I provides that parties shall –

- endeavour to remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives;
- shall avoid locating military objectives within or near densely populated areas; and
- shall take the other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations.

While Russia achieved its military objective in Ukraine, namely to create a separatist region, Novorossiya, its failure was in the way it was unable to bring together its diverse hybrid methods to achieve political success in terms of public acceptance of its operations at present and overall legitimacy in the future. Here Putin signally failed.[19]

Cyberattacks and the information sphere

The actual risk of a state-originated cyberattack against the United Kingdom or another member of NATO is unknown but, as Russia has cyber capability, the authors assess this risk as potentially medium to high.

Cyberattacks which resemble examples of the fifth dimension of warfare, refer to a sustained campaign of concerted cyber operations against the information technology (IT) infrastructure of the targeted state, including and leading to mass web destruction, spam and malware infection.[20]

The almost ubiquitous access to the Internet, and the interconnectivity of critical systems, makes this form of hybrid warfare a serious and very real threat. The effectiveness of cyberattack was graphically demonstrated by the sophisticated Stuxnet virus attack on the Iranian nuclear plants. Stuxnet was described as –

> [O]ne of the most sophisticated pieces of malware ever detected [and] was probably targeting 'high value' infrastructure in Iran … It is believed to be the first-known worm designed to target real-world infrastructure such as power stations, water plants and industrial units.[21]

Stuxnet has also been described as "the world's first digital weapon".[22] This cyberattack was also a clear demonstration of the difficulty of attribution. While there were suspicions about which nations in the world possessed the technical competence to develop and insinuate such a worm, there was insufficient proof. It consisted of –

> [A] 500-kilobyte computer worm that infected the software of at least 14 industrial sites in Iran, including a uranium-enrichment plant. Although a computer virus relies on an unwitting victim to install it, a worm spreads on its own, often over a computer network.[23]

Cyber-conflict and cyber-warfare are great examples of the use of new technologies within the scope of hybrid threats. The combination of new technology and its availability make cyber-supported or cyber-led hybrid threats potent. Cyber threats strike at the core of modern war-fighting by affecting command and control abilities, which have become vulnerable to such cyberattacks. In an age of autonomous weapons systems, such as unmanned aerial vehicles (drones) and robot fighting vehicles, the potential for cyber intervention into their control systems is no theoretical possibility. If the security systems safeguarding the autonomous technology can be overridden by hackers, it could cause havoc on the battle field: UK weapons targeting an enemy could be turned on British soldiers. The concerns of "hijacking risks" were articulated by Huw Williams, editor of *IHS Jane's International Defence Review*, who said, "It remains a concern, no encryption is perfect and there is still the danger that a data link can be broken." Hijacking risks will increase as the system becomes more automated, regardless of whether the platform is still controlled by a human operator.[24]

Russia has been one of the most prolific users of cyber capabilities, and its use of cyberattacks against states has been well documented in the past: 2007 Estonia and 2008 Georgia and now the ongoing cyber operations targeting critical infrastructure in Ukraine.[25] In 2007, Russia attempted to disrupt Estonia's Internet infrastructure as retribution for the country's removal of a WWII Soviet War Memorial from the centre of Tallinn. Russia also augmented its conventional military campaign in Georgia with cyber capabilities, which severely hampered the functioning of government and business websites.

These cyberattacks are being supported by the use of the information sphere where misinformation and propaganda are being used to complement the overall Russian-integrated approach to hybrid warfare. Russia uses the media, for example, *Russia Today*, *Sputnik News*, and members of the public sympathetic to Russia who write to newspapers, to spread propaganda and misinformation in a highly persuasive and credible way.

In the present conflict in Eastern Ukraine, Russia has effectively used the information sphere as an integral tool in its hybrid war against the people of Ukraine

Vulnerability and dependency of essential services, key infrastructure and utilities

Permitting the sale of essential services and key infrastructure such as airports, power stations and other strategic resources such as steel and coal to 'foreign', non-citizen, private and legal owners, lays open a vulnerability to potential shutdown and/or dependency thus creating a medium to high risk scenario.

In 2015, the Russian president threatened to cut the vital gas supply to Western Europe through Ukraine if financial demands made by Gazprom to Ukraine were not met.[26] This threat reminded the European Union (EU) of its dependency on Russian gas deliveries and also served as a warning not to confront Russia's aggression in East Ukraine. While this incident has to be seen as directly linked to the Russian–Ukrainian conflict it also serves as a sombre warning of what to expect from Russia in instances of future disagreement and diplomatic/political confrontation. Some nations have seen foreign takeovers as a security threat and have taken direct action.[27] Russian billionaires have reportedly gained major interests in Europe and North America, controlling organisations like football clubs, and huge, under-the-public-radar industrial groups.[28] In 2015, the UK prime minister blocked a deal that could have seen "a group of Russian oligarchs led by Mikhail Fridman from seizing control of 12 North Sea gas fields".[29] In 2014, Heathrow Airport Holdings sold three British airports to foreign buyers in a £1 billion deal.[30] In 2012, the Daily Mail columnist, Alex Brummer, voiced the question, "… what happens when most of Britain's essential public services are no longer run by the British? […] Roughly half of all our essential services – from water to bridges and ports – now have overseas owners." The state-owned Russian gas conglomerate Gazprom had expressed an interest in –

> British Gas's parent company Centrica, gaining access to its 15.7 million UK customers. At the time, the Kremlin was using its huge energy resources as a political weapon by turning off gas taps supplying the Ukraine. If they could do it to the Ukraine, some feared, there was nothing to prevent them doing it to us one day. […] many breathed a sigh of relief when Gazprom dropped the idea of making an official bid. As former Chancellor Alastair Darling remarked: 'There's a huge issue and it's [sic] security. Frankly, as we know, if you lose power it is catastrophic. Remember the blackout in London a few years ago? It was an accident but it paralysed half the City and it was terrifying.'[31]

While this was a direct approach, it is possible to conceal a company's true identity through a myriad of subsidiary companies.

There are similar risks about the nuclear industry. Britain's nuclear power-generating plants are controlled by French state energy giant EDF. In October 2015, EDF agreed a deal under which China General Nuclear Power Corporation (CGN) would pay a third of the cost of the £18 billion project for Hinckley Point in exchange for a 33.5% stake.[32] Four of the big six energy companies, including most of the nuclear industry, are foreign-owned. The same goes for British seaports, airports and railways.[33]

These dependencies are being increased by Europe's overall dependency on foreign energy producers and suppliers.[34] This dependency of importing energy is a crucial weakness of European energy policies[35] and is amplified by Germany's decision to phase out nuclear power by 2022.[36] Chancellor Merkel's ill-thought decision in 2011 does make Germany, as the European Union's biggest economy, even more dependent on Russian energy. The same applies to the European Union, given its interdependent and shared power transmission grids.

Electronic warfare

Russia has a sophisticate electronic warfare capability. Lt Gen. Ben Hodges, the US Army's most senior commander in Europe has described the quality and sophistication of their electronic warfare as "eye watering".[37] He noted Russia's modernised jamming and signal direction-finding capabilities and outlined that, in Eastern Ukraine, Russian-backed forces employed jammers to interfere with drones, which the Organization for Security and Cooperation in Europe intended to use for monitoring compliance with the Minsk cease-fire agreement. "Ukraine's ground defense systems are being jammed, creating what is essentially a 'no-fly zone.'"[38]

Espionage

Russia has a well-organised and professional intelligence agency and spy network throughout the world. Its activities in London are a matter of public record.[39] It has operated in the United Kingdom for some time. The notorious 'Cambridge Spy Ring', known by the KGB as the 'magnificent five',[40] was a cancer at the heart of the UK intelligence service and operated from the late 1930s. For the Russians, they were a very successful source of intelligence. "All the Cambridge spies caused damage to their country … Philby's contribution was more poisonous. He betrayed the names of as many British agents as he could, including lists of all those who had spied for us in Nazi-occupied eastern Europe."[41] That Russia took espionage very seriously was evidenced by the fact that, by the 1950s, KGB operatives and spies were outnumbering MI5 officers by more than three to one.[42]

Russia's 'spying' activities are both overt – in the sense that aircraft intruding into UK airspace are not easily concealed[43] – and covert. The presence of Russian agents and their methods has been brought once more into sharp focus by the murder of Alexander Litvinenko, with one newspaper reporting that the "[n]umber of Russian spies in the UK is back to Cold War levels, say security services".[44] Espionage is not confined to obtaining military information only but also commercial knowledge and plans.

Methods vary from eavesdropping through the use of 'bugs' and surveillance devices, to the 'honey trap', whereby a young male or female forms an intimate relationship with a 'target' individual identified as useful for his or her contacts, then uses that relationship to insinuate himself/herself into closer ties with those contacts, some of whom may be identified as high value, e.g. senior scientists, government ministers or senior members of the military.

While the operations of the intelligence services have the legal constraints of the Regulation of Investigatory Powers Act 2000, the Intelligence Services Act 1994 and copious anti-terror legislation,[45] Russian agents operating in the UK do not. They can employ intrusive surveillance methods without the same constraints. Their accountability is to their superiors in the intelligence service and the military, in accordance with the Law on Foreign Intelligence 1992 and the Law on Foreign Intelligence Organs 1995.[46] This latter provision covers the conduct of electronic surveillance in foreign countries.

Other methods use respectable sounding organisations as a front for more sinister activity. The Haldane Society of Socialist Lawyers remained affiliated to

the International Association of Democratic Lawyers during a period in which it was an international front organisation of Soviet intelligence services.[47]

Russia has also used infiltration, as described in the section on migration, to embed agents. From the end of the 1980s, the KGB and later the SVR (Russia's external intelligence service) began to create "a second echelon" of "auxiliary agents in addition to our main weapons, illegals and special agents".[48] These agents comprised legal immigrants, including scientists and other professionals. Another SVR officer who defected to Britain in 1996 described details about a thousand Russian agents and intelligence officers, some of them "illegals" who live under deep cover abroad.[49] Recently caught Russian high-profile agents in the United States are Aldrich Hazen Ames, Harold James Nicholson, Earl Edwin Pitts, Robert Philip Hanssen and George Trofimoff.

Mass migration and hybrid war

Mass migration, strategically designed and used, has the potential to undermine European identity and security. Migration-aided coercion was already used by the ousted Libyan dictator, Moammar Gadhafi, to force a lifting of European economic sanctions in 2004. Whether the Turkish President Recep Tayyip Erdogan employed the same tactic in order to receive direct funds from the EU remains to be discussed. What could be established at the time of the writing of the article was the growing dependency of Europe on Erdogan's willingness to act as a trustworthy partner. His announcement in the autumn of 2016 to 'flood' Europe with migrants resembles a 'weaponisation' of the migration crisis in terms of a hybrid threat scenario.[50] The decision by Germany's Chancellor Angela Merkel, to disregard applicable European law (Schengen and Dublin), when she decided to grant Syrians generally asylum status, led to a split within the European Union and to diplomatic upsets in the affected EU countries. Mass migration has the potential to be used as a geo-strategic weapon: State and non-state actors propose deriving financial and political capital out of this situation. This is underpinned by the legal requirement for state parties to the 1951 UN Convention Relating to the Status of Refugees to accept those who are fleeing political or other forms of persecution (race, religion, nationality, membership of a particular social group or political opinion).

The protection of national borders within the framework of national and supranational jurisdiction (Schengen) is a necessary condition of state sovereignty. Neglecting this international legal principle leads to an erosion of national sovereignty and identity, just as the terrorist attacks in Paris during November 2015

illustrate the dangers of deterioration of European border controls, partly caused by Germany's migration policy neglect. Both EU and national border controls have absolute priority to restrict terrorists in their freedom of movement. Without adequate concerted action, the EU principle of free movement of persons is permanently eroded.[51]

The UK's laudable adherence to human rights is one such area where its strength is, paradoxically, also its weakness. There are two main human rights documents of relevance: The Human Rights Act 1998 [52] and the European Convention on Human Rights (ECHR).[53] These two legal documents provide a framework within which UK laws and individual rights are applied and enjoyed, guaranteeing basic freedoms, such as the right to life, the prohibition on torture, the right to family life.

In addition, the United Kingdom has ratified the –

- Convention and Protocol Relating to the Status of Refugees (Refugee Convention);[54]
- International Covenant on Civil and Political Rights (UN ICCPR);[55]
- United Nations Convention Against Torture (UNCAT);[56]
- Convention on the Rights of the Child 1990[57] (The most important of which is the Article 6 right to life, survival and development); and
- Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict.[58]

In each of these legal documents, there is an onus placed upon each signatory state to implement the protections set out. In turn, this means that the government is exposed to the prospect of litigation, which, as one sees in the case of the United Kingdom, is usually through the medium of the Human Rights Act of 1998 and ECHR. Under the Convention of the Rights of a Child of 1990, in combination with Article 8 of the ECHR (the right to family life), the parents of children provided with sanctuary in the United Kingdom are able to seek entry to the United Kingdom to be with their children. The misuse of this provision, by sending children on ahead, would provide an avenue for terrorist and undesirable elements to enter the country.

It has been suggested that –

> [M]ass migration has the potential to become a hybrid threat exploited by state and non-state-actors in order to make Islamist terrorism a real hybrid threat. […] Migration aided coercion was already used by the ousted Libyan dictator Moammar al Gadhafi, to force a lifting of European economic sanctions in 2004.[59]

Using population displacement as a form of warfare, such as that graphically shown by the internal armed conflict in Syria, serves two purposes: it overwhelms an enemy with the sheer volume of displaced persons, causing internal dissent as to how the matter should be resolved and, simultaneously, provides an avenue for the infiltration of militants[60] who may benefit from the inability to employ efficient and rigorous document checks to ascertain the bona fides of each entrant. This idea has been described as "stealth jihad".[61]

The situation was serious enough for Pope Francis to express his own concerns that ISIS jihadists were 'infiltrating' Europe through the refugee crisis,[62] and is a 'Trojan Horse'-like deception to undermine Western societies. More recently, the journalist Con Coughlin wrote along similar lines that the so-called Islamic State "terrorist group is exploiting an unprecedented refugee crisis and the flames of intolerance it fans to infiltrate European civilisation".[63] As he tellingly pointed out, "with an estimated 1.5 million refugees said to have entered the EU in 2015 … it is virtually impossible to undertake effective scrutiny of everyone entering the mainland".[64] The overwhelming numbers did not permit proper investigation of the bona fides of each person presenting as a refugee. Nearly all were treated as refugees. Yet, large numbers of single, young men, some with a distinctly different ethnic appearance to Syrians, were being admitted without demur.

Large-scale migration can then engender internal discord between those focusing on the security threat to the nation and those more focused on the humanitarian problem, which, in itself, will be widely reported on by press and TV. Internally, the state will find its support structures seriously challenged. As Migration Watch[65] points out, pressures will be placed on housing, schools, medical facilities and welfare benefits. Local citizens, who are on council waiting lists for housing, may find themselves displaced in the queue by migrants, who are given higher priority.[66] The fact that such attitudes by local officials cause unrest and anti-immigrant sentiment is another hybrid factor.

These attitudes are exacerbated by instances where migrants do not adapt to their host communities by either refusing to accept the indigenous culture and values or not understanding how their own values are subordinate to those of their new home, whether or not they agree with them. The most egregious examples of this cultural clash are illustrated in the sexual assaults on women and children, which have occurred in the United Kingdom and Europe.[67]

For Europe, this has presented a crisis for the parties to the Schengen Agreement,[68] with even Germany reintroducing border controls and checks[69] –

supported by some, but criticised by other citizens. The European Union seems close to accepting that its "Schengen open-borders area may be suspended for up to two years if it fails in the next few weeks to curb the influx of migrants from the Middle East and Africa". Austrian Interior Minister Johanna Mikl-Leitner, whose government has warned it will limit entry to migrants has said, "[e]veryone understands that the Schengen zone is on the brink. If we cannot protect the external EU border, the Greek-Turkish border, then the Schengen external border will move towards central Europe … Greece must … accept help."[70]

These are uncomfortable ideas and the very fact they are regarded as such, and that anyone publicly voicing concerns about them might be loudly vilified, is another hybrid area of potential exploitation, to dumb-down criticism and opposition to the means employed.

It has been said that President Putin's "current aim is to foster the European Union's disintegration, and the best way to do so is to flood the European Union with Syrian refugees".[71] If this is true, then Russia is using the powerful dynamic of Syrian population displacement as a means of hybrid warfare in the context of undermining the European Union. Some might say that the referendum decision of UK voters, on 23 June 2016, to leave the EU is helping achieve that purpose.

Lawfare as a strategy of hybrid warfare

Lawfare is using law as a weapon with a goal of manipulating the law by changing legal paradigms.[72] Lawfare can be defined "[as] the strategy of using - or misusing - law as a substitute for traditional military means to achieve an operational objective".[73] In the case of the current situation in Russia and Ukraine, lawfare has its roots in an undefined situation, i.e. the lack of definition of the conflict – international armed conflict, non-international armed conflict, or civil unrest. This ambiguous situation creates patent confusion as to the source or paradigm of applicable law and any eventual action to identify and assign legal responsibilities and demand accountability. The aim is to deny the existence of the roots, causes and realities of the Russian operations in Crimea and Eastern Ukraine, This deniability of reality in fact gives the Western nations the possibility to avoid taking responsibility by deferring a decision on the grounds that the situation in Eastern Ukraine was not independently verified, that no Russian direct involvement was evident, etc. This deniability (often supported by acts of disinformation), the lack of definition of the conflict – international armed conflict, non-international armed conflict, or civil unrest – make it hard to qualify the nature of the conflict and with it to agree on the appropriate course of action in response.

Lawfare in the context of the Russo–Ukrainian conflict and Syria can be used to camouflage the role the parties play in the conflict. This might take the form of state-to-state aggression behind the mantle of a "humanitarian intervention".[74] This is the use of "humanitarian intervention" as an excuse to intervene in the sovereign affairs of a third-party state. Unilateral action on the part of powerful states who purport to cloak themselves superficially in the UN Charter as a justification for what they do, has the potential to lower the threshold for conflict with those who see things differently. While it is clearly prepared to take steps to protect its sphere of influence, as it did recently in Georgia/Ossetia, Crimea, Ukraine/Donbas, Russia has shown little appetite for military adventurism further afield. It abstained in the UN Security Council over the vote on Libya and, having seen how things turned out, in the way the mandate was interpreted and implemented as a tool for regime change, it has publicly stated it will not support any resolution which calls for the use of force in Syria. Its current operations in Syria are in aid of the government, a close ally and a country where it has a keen strategic interest, particularly in relation to the naval base at Tartus. Consequently, it is not really fighting a proxy war there. However, Saudi Arabia and Iran are. The Saudis, Qataris and Turks have armed and supplied the Islamist rebels opposed to President Assad, and the Iranians have assisted the government and provided military personnel. The United States has reputedly assisted both the 'rebels' and the government – the CIA have given 'technical assistance' to the rebels, some of whom are anything but secular, and the US army has provided "US intelligence to the militaries of other nations, on the understanding that it would be passed on to the Syrian army and used against the common enemy, Jabhat al-Nusra and Islamic State, to the government."[75]

Allied to this use of 'lawfare' within the context of international law is the context of UK military involvement in operations in Iraq and Afghanistan, where claims to UK courts alleging breaches of human rights by members of the armed forces were and are being submitted. The expense[76] and volume of claims have the ability to –

- Portray the UK's servicemen and women in an adverse light, thereby lowering them in the esteem of the public. This could have an influence upon recruiting – who would want to join an organisation that disrespects human rights?
- Have a wider negative propaganda effect outside of the United Kingdom, again affecting the United Kingdom's reputation;

- Tie up the Ministry of Defence for months and even years, responding to these claims;[77]
- Affect the operational effectiveness of the military adversely by leaving few options open (Serdar Mohammed);[78]
- Affect morale in the armed forces adversely with the concern that every aspect of a serviceman's conduct will be open to scrutiny. This is believed may cause them to hesitate to act when decisive action is required; [79]
- Effect the slow drip of the operational modus operandi and intelligence into the public arena, by which an enemy understands restrictions/limitations placed upon the force, which it can then exploit; and
- Damage the 'control principle' by which classified intelligence is imparted by a second nation to assist with our national security on the strict understanding it is not disclosed without the consent of that second nation (Binyam Mohammed[80]).

The process has been described frankly as "legal mission creep" abetted by "significant judicial figures" who "give little or no hint of any pull back by the Bench from the 'judicialisation of war'".[81]

One of the very principles of which the United Kingdom has a proud tradition and which it champions throughout the world is, conversely, a vulnerability as a form of lawfare. It raises the question whether UK laws permit sufficient flexibility to react swiftly to all of the varied forms hybrid attacks might take. The very nature of a tolerant society is open to exploitation and abuse through the championing of division and heightening ethnic and racial tensions. As has been said, "[t]he fundamental characteristic of hybrid attack is that it is designed to exploit a country's vulnerabilities".[82]

This can also be augmented by lawfare using the ECHR and democratic legal processes to place financial burdens on legal systems by challenging decisions on, for example, asylum status, conditions of housing, payable benefits, religious freedoms, and using anti-discrimination laws to influence societal attitudes. It may also be used by militants who claim they will suffer persecution if returned to their home country, or by captured terrorists who want to resist being handed over to their state detention authorities. In the egregious case of Serdar Mohammed, English courts have been used by a Taliban commander whose organisation was trying to kill British soldiers to claim compensation from the

United Kingdom for his detention. As pointed out at paragraph 21 of the judgment of the Court of Appeal in the case of Serdar Mohammed, [83] there are hundreds of cases arising out of the acts of British servicemen in Iraq – and Afghanistan – which are awaiting hearing and which have the potential to burden the judicial – and legal aid – system for some time, at significant cost to the British taxpayer.[84]

Lawfare may be used a means of exploiting the genuine misery and suffering of many, for a political or military goal, by creating conditions that make life so unbearable where they are, that families uproot and move to safety. That crisis may also be used to infiltrate combatants into the destination country.

The risk for the United Kingdom is high. The threat is on going and, even if not directly employed by any particular state, is nevertheless something from which an interested party can derive a benefit.

The challenges: Whether to respond and, if so, how to respond

This section examines the applicable law, what constitutes an armed attack, the threshold for a response and how that response might be delivered.

International law

As a member of NATO, any attack upon the United Kingdom would invoke Article 5 of the NATO Treaty.[85] Importantly, for the purpose of Article 6, an armed attack on one or more of the parties is deemed to include an armed attack on the territory of any of the parties and on the forces, vessels, or aircraft of any of the parties. Unfortunately, the term 'armed attack' is not defined. But it was considered in the case of Nicaragua v. United States (1987)[86] when it was stated, at para 195, that the nature of acts, which can be treated as constituting armed attacks include not merely action by regular armed forces across an international border, but also "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to" (inter alia) an actual armed attack conducted by regular forces, "or its substantial involvement therein".

The Court went on to consider the position of assistance by third-party states to rebels in the form of the provision of weapons or logistical or other support, which it said constituted "a threat or use of force, or amount to intervention in the internal or external affairs of other States".

The "[d]efinition has been given new life by becoming a major source for the negotiations on the definition of the crime of aggression within the jurisdiction

of the International Criminal Court". Drawing upon the General Assembly resolution 3314 (XXIX),[87] the Rome Statute of the International Criminal Court on the crime of aggression defined in its Article 8 *bis* (1) a "crime of aggression" as

> the planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political or military action of a State, of an act of aggression which, by its character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations.[88]

The threshold requirement is that the act of aggression must constitute a manifest violation of the Charter of the United Nations in the use of armed force by a state against the sovereignty, territorial integrity or political independence of another state, or in any other manner inconsistent with the Charter of the United Nations.

An "act of aggression" was itself defined as including the use of armed force in any manner inconsistent with the UN Charter, whether or not there is an actual declaration of war. It is interesting that the list of activities that qualify as an act of aggression does not specifically refer to cyberattacks that have such serious consequences, although there is reference to "the use of any weapons by a State against the territory of another State".[89]

Under international law, a nation is entitled to use force in three situations:

- When it is authorised by the United Nations Security Council, pursuant to Article 2(4)[90] and (7)[91] of the UN Charter;
- In self-defence of itself, under Article 51[92] of the UN Charter; and
- In response to the lawful request by the government of an ally for assistance, or collective self-defence (as per the NATO Treaty) also under Article 51 (and a matter of customary law).

Where action is taken under Article 51, in the exercise of the right of self-defence, it "shall be immediately reported to the Security Council". If armed force is used to respond to an attack, then it must be in keeping with International Humanitarian Law, that is, it must not be expected "to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated".[93]

The Nicaragua judgment sets out very helpful guidance on the definition of 'armed attack' and 'aggression'. It is therefore important to consider how this

translates into acts which are less easy to identify as a use of force, such as cyberattacks. It is suggested that disruption of a military national defence facility could easily cross the threshold where, for example, national air defence systems are disabled. But, an attack disabling the banking system, while disruptive, may not. Other problems relate to what the status is of civilians involved in cyberattacks, and which implications cyber offences can have for neutral states.[94]

Whether any form of hybrid attack, alone or cumulatively, amounts to a use of force and, if so, reaches the threshold of an 'armed attack' to justify a military response under article 51 – and what form that response would take – are very difficult questions to answer. They are situation/fact-specific. Moreover, attribution is likely to be very problematic. Devastating cyber infiltration can be achieved by a single operator who would be difficult to track and it would be even more difficult to lay attribution to any particular state. In relation to the Stuxnet worm, while very few nations had the level of expertise necessary to produce such a virus, direct attribution has remained elusive.[95]

The Tallinn Manual[96] discusses the legal framework applicable to cyber-warfare and, in particular, what constitutes a use of force (rule 11), what constitutes a threat of force (rule 12), the permissible responses (rules 13–15), based upon Article 51 of the UN Charter, and the applicability of the law of armed conflict (Part II).

Rule 11 defines a cyber operation as constituting a use of force when its scale and effect are comparable to non-cyber operations rising to the level of a use of force. This is not limited to the use of such means by the military but would also include, for example, the intelligence services, under the principles of state responsibility and attribution.[97] *A fortiori*, if conduct is directed or controlled by a state.[98] However, according to the commentary to rule 11 of Tallinn (use of force), "non-destructive cyber psychological operations intended solely to undermine confidence in a government or economy do not qualify as uses of force" (ibid., §3),

Moreover, "merely funding a hacktivist group conducting cyber operations as part of an insurgency would not be a use of force". The authors consider that, under the principles of the Nicaragua case, "providing an organised group with malware and the training necessary to use it to carry out cyber attacks against another state" (ibid., §4) would constitute a use of force.

In considering whether an act constitutes a 'use of force' and amounts to an 'armed attack' the authors determined that the Nicaragua judgment set out the applicable criteria. (ibid., §6).

Tallinn acknowledges that the question of what actions short of an armed attack constitute a use of force is still unresolved (ibid., §8). Where the harm caused is significant (rule 13), then there is clearly an armed attack. This is, however, still an evolving area of law and it is difficult to assess what a given nation would regard as 'significant' for the purposes of such a classification. Even assuming that the threshold has been met, a response will also depend upon whether the nation attacked has the capability to respond militarily or via other means. While cyber responses can be an effective option in self-defence, the problem of accurate attribution remains. The elements of an internationally wrongful act of a state are set out in Article 2 of the Responsibility of States for Internationally Wrongful Acts, 2001. This provides,

> There is an internationally wrongful act of a state when conduct consisting of an action or omission:
>
> (a) is attributable to the state under international law; and
>
> (b) constitutes a breach of an international obligation of the state.

As a matter of pragmatism, it is suggested that attribution requires absolutely incontrovertible proof that an attack emanated from a specific country, from its military or government departments, and that it was of such a nature as to cross the legal threshold, any response could be itself construed as an act of aggression. How does one decide that it is an official act of state, conducted by organs of a state[99] and not some rogue computer boffin with access to an official computer who has, for example, decided to hack into the another nation's missile defence system and disable it? To the observer, this use of an official government computer would look like a genuine cyberattack by the state from which it originated.

On the other hand, what should the targeted state do when the state from which the attack originates denies that it was the act of any of its officials, even though it is *suspected* by the victim state that this is untrue? This is ostensibly an act of state, but is pleaded to be by a rogue and unauthorised element, acting without authority. It is quite different to the situation of, for example, a missile launch. First, such weapons system would be under control of the state's military and access to them is severely restricted. Secondly, a rogue soldier operator of the system cannot easily initiate an attack sequence without attracting serious attention. The more powerful the weapon, the more controls there are over it. Hence, the explanation for the cyberattack may be considered more credible.

Matters are even further complicated where, for example, a particular system, e.g. missile defence, is placed under the authority or control of another state.[100] In those circumstances, the rules state,

> [T]he conduct of an organ placed at the disposal of a State by another State shall be considered an act of the former State under international law if the organ is acting in the exercise of elements of the governmental authority of the State at whose disposal it is placed.[101]

In his article, "Historical background and development of codification", Crawford has said,

> [T]he right to invoke responsibility is not necessarily co-extensive with the circumstance of being the victim of the breach of an international obligation: the injured State may not be the only one entitled to invoke responsibility for an internationally wrongful act, although injured States *should* retain priority in terms of any response.[102] [emphasis added]

In the context of foreign ownership of essential utilities, e.g. the planned nuclear power installation at Hinkley Point, the construction costs for which will be paid for by the mainly state-owned EDF of France and state-owned CGN of China,[103] an attack on such installations may indeed prove to be so significant as to constitute an armed attack. While the state on whose territory the installation is based (United Kingdom) may, for whatever reason, deem it imprudent to make a military response, is the nation which has invested financially in it constrained by that view? Does the loss of its significant and expensive investment mean it, too, is it an 'injured state'?

It is always open to a state to choose to respond in self-defence if it perceives the threshold for an armed attack upon it has occurred, but within the framework of significant hybrid attacks the problem of attribution remains challenging.

Conclusion

Russia has been carrying out espionage for many years, and regularly tests UK defences. Nevertheless, it has not displayed any intent to attack the United Kingdom by conventional means. UK membership of NATO may be a key factor in this, or it may be just coincidental, as it is far from Russian borders. Or simply, Russia has nothing to gain from such a move given its elites' interests and presence in the UK's public life, educational system and economy?

Therefore, a major question still to be decided is how much of a real threat it is to the United Kingdom in general. It is doubtful that Russia's hostile interest extends as far as the United Kingdom, as its traditional sphere has been with its neighbouring countries which provided it with a security buffer. Having said that, one might argue that Russian operations in Syria show that it casts a predatory eye much further afield. But, this is to be seen from the perspective of assistance to its Syrian ally, and where it has genuine interests of its own. Russia's operations there, to aid its ally the Syrian government, were not a direct threat to Western interests and, far from much of the criticism directed to it, are quite understandable in that context. In contrast, Syria is of strategic importance to Russia and there is also the serious threat of Islamic terrorism so close to its borders, which is of genuine concern to the Kremlin.[104] Russian involvement in Syria has been described often pejoratively by Western media and policymakers as an intervention.[105] This is incorrect, as Russia has come lawfully to the assistance of an ally that has faced internal and, to a considerable extent, external threats. Its operations in Syria are therefore with the consent of the Syrian government. This is in stark contrast to the involvement there of other nations who have allied with, and/or provided assistance to, militants fighting the government.

As was pointed out in the *New York Times*, "The liberal interventionists … seem to have forgotten that Syria has been Moscow's client since early in the Cold War – a situation Washington was willing to live with when the geostrategic stakes were much higher."[106]

The events in Crimea (home to the Russian Black Sea Fleet) and Ukraine (sharing a common history, home to many Russians and Russian speakers), similar to the situation in South Ossetia and Abkhazia, are illustrative of Russia's assertion of its right to defend its 'citizens' abroad, and tend to be more easily understood if seen through that prism, so that the vulnerability of these states to the Russian bear is more easily comprehended. That is not to justify what happened, but merely to understand why it did.

All the same, events in Crimea and Ukraine have shown how the UK government must become "alert to the use of reflexive control techniques and find ways to counter them if [we are] to succeed in an era of hybrid war".[107] They have been useful in highlighting the limitations of hybrid warfare. In East Ukraine, Russia combined 'little green men' and virulent propaganda against the government in Kiev. However, Galeotti points out –

> The very disarray in Kiev, which had worked to Moscow's advantage over Crimea, now proved a serious problem, as there was no one there able or

> willing to make the kind of politically ruinous concessions the Russians were demanding. Instead, a 'short, victorious little war' … turned into a 'bleeding wound'…[108]

What these events reveal is that Russia will defend its geostrategic interests. But that is quite different to openly attacking a country like the United Kingdom, which is far removed from Russia's sphere of interest as it sits firmly within NATO. So, direct use of force against the United Kingdom is currently assessed as highly unlikely.

Notwithstanding the absence of any perceived hostile intent for a conventional attack, hybrid warfare offers Russia more subtle ways of undermining British society and values. The distinct advantages of cyber warfare are all too apparent, as attribution is very difficult. Six years after Stuxnet, there is still no direct attribution, even though the capability to produce such a sophisticated program resides with only a small number of nations and organisations.

General Valery Gerasimov was quite clear when, drawing upon the lessons of the so-called Arab Spring, he said, "The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness."[109]

Galeotti candidly added the rider,

> In other words, this is an explicit recognition not only that all conflicts are actually means to political ends – the actual forces used are irrelevant – but that in the modern realities, Russia must look to non-military instruments increasingly.[110]

It is clear that Russia has successfully employed several hybrid methods of warfare in recent times, and that it is skilled in so doing. It has also successfully employed conventional forces in Syria, which have changed the course of the civil war in favour of President Assad. Its prowess and confidence have grown. In response, NATO has deployed a missile shield to Poland and Romania, to deter any resurgent and over-confident military move by Russia. In turn, Russia has deployed Iskander missiles to Kaliningrad, the Russian territory between Poland and Lithuania that is the most militarised zone in Europe.[111] This military posturing may itself be a form of hybrid warfare, as he who 'blinks first' will be regarded as the weaker party. The danger is if this face-off escalates, direct conflict may become more likely.

While the United Kingdom may not be under imminent threat of traditional armed attack from Russia, it must defend against the sub-threshold corrosion

evident through espionage, propaganda and disinformation, that gnaws away and undermines its security and society, and ensure that any responses are measured and in accordance with international law.

At a more strategic level, governments have tried to make predictions on the future threats they will face, and produced commensurate defence assessments – in the case of the United Kingdom, to reduce its conventional forces. The public has been fed platitudes about leaner and more efficient forces, as a euphemism for cost-cutting. This has been wrong and has, as a result, placed the nation at dangerously low force levels, purporting to identify new threats, which diminish the importance of more conventional forces.[112] While some of this thinking is driven by national austerity measures, the absence of any senior government figure who has experienced the rigours of combat plays a significant part too, as there is a signal lack of appreciation of what is needed to produce an efficient and capable force.[113] Indeed, that lack of military acumen is, in itself, a potential hybrid threat, which an enemy could exploit.

In truth, there is no single type of threat that the nation faces, nor does each threat stand in isolation. Hybrid warfare can mix and match the obvious with the most subtle. What Russia's interventions in Crimea and East Ukraine have shown is that there are many and varied challenges to be met, in addition to the conventional threat. The United Kingdom must have the force levels to meet them and the capability to work in an integrated way with its national security agencies and strategic allies.

Endnotes

---

[1] *Dr.Sascha-Dominik (Dov) Bachmann*, Assessor Jur, LLM (Stel) LLD (UJ), is an Associate Professor in International Law (Bournemouth University, UK) and extraordinary Associate Professor in War Studies (Swedish Defence University, SWE). Outside academics, he served in various capacities as lieutenant colonel (army reserve), taking part in peacekeeping missions in operational and advisory capacities The author took part as NATO's Rule of Law Subject Matter Expert (SME) in NATO's Hybrid Threat Experiment of 2011 and in related workshops at NATO and national level. sbachmann@bournemouth.ac.uk.

[2] *Brigadier (rtd) Anthony Paphiti* read law at the University of Leeds and subsequently qualified as a barrister in 1975 (Inner Temple). He practised at the Bar in London until joining the UK army in 1981 as a legal officer. During that time he served as a prosecutor and spent 4 years with NATO, as the first legal adviser to HQ ARRC and then C-SPT in Zagreb, before

eventually taking over as the day-to-day head of the Army Prosecuting Authority. He retired from the army in 2006 and returned to practice in criminal law, until setting up the *Aspals* Consultancy in 2008, which specialises in Military and International Law. He is the author of the *Military Justice Handbook, for Court-Martial Practitioners*, published in 2013.

[3] Bachmann, S-D & Gunneriusson, H. "Hybrid wars: The 21st century's new threats to global peace and security". *Scientia Militaria* 43/1. 2015. 77–98.

[4] Calha, JM."Hybrid warfare: NATO's new strategic challenge?" NATO. 7 April 2015. < http://www.nato-pa.int/Default.asp?CAT2=3924&CAT1=16&CAT0=2&COM=4018&MOD=0&SMD=0&SSMD=0&STA=0&ID=0&PAR=0&LNG=0> Accessed on 20 December 2016.

[5] Gerasimov, V. "The value of science in prediction". <https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/> Accessed on 20 December 2016.

[6] Hoffman, FG. "Hybrid threats: Reconceptualizing the evolving character of modern conflict". *Strategic Forum* No. 240. 2009. 1; also see Hoffman, FG "Hybrid warfare and challenges". *Joint Forces Quarterly* 52.1 Q. 2009. 1–2; Hoffman, FG. "Hybrid vs. compound war: The Janus choice of modern war: Defining today's multifaceted conflict". *Armed Forces Journal* October 2009. 1–2; and the seminal work on the topic, see Hoffman, FG *Conflict in the 21st century – the rise of hybrid wars*. Arlington, VA: Potomac Institute for Policy Studies, 2007, 37.

[7] NATO ACT. "NATO Countering the Hybrid Threat". NATO < http://www.act.nato.int/nato-countering-the-hybrid-threat > Accessed on 20 December 2016.

[8] *Cf*. Bachmann, S-D. "Hybride Bedrohungen". In Österreichisches Bundesheer (Austrian Army), *Sicher und Morgen? Sicherheits Politische Jahresvorschau 2016* (Security Political Preview for 2016), 85–87. <http://www.ooe.bundesheer.at/pdf_pool/publikationen/sipol_jvs2016.pdf> Accessed on 20 December 2016.

[9] Deep, A. "Hybrid war: Old concept, new techniques". *Small Wars Journal*, 2 March 2015, cited in Mosquera, A. & Bachmann, S-D. "Hybrid warfare and lawfare". *The Operational Law Quarterly* 16/1. 2015, 2-5.

[10] "The Soviets were given inside secrets on the development of Concorde by a spy codenamed 'Ace', according to new revelations ... The agent was just one of more than a dozen spies operating within Britain and passing commercial and technological secrets to the Russians at the height of the Cold War ...". BBC Unattributed. "UK Politics - 'Ace' spy revealed Concorde secrets". *BBC News.* 14 September 1999. <http://news.bbc.co.uk/2/hi/uk_news/politics/447464.stm> Accessed on 20 December 2016. See also Klein,C. "The Cold War race to build the Concorde". 21 January 2016. <http://www.history.com/news/the-cold-war-race-to-build-the-concorde> Accessed on 20 December 2016. For an

interesting discussion on the background to this rivalry, see the transcript of the programme entitled "Supersonic Spies" on *PBS*, aired on 27 January 1998: <http://www.pbs.org/wgbh/nova/transcripts/2503supersonic.html> Accessed on 20 December 2016.

[11] NATO, "Keynote speech by NATO Secretary General Jens Stoltenberg at the opening of the NATO Transformation Seminar < http://www.nato.int/cps/en/natohq/opinions_118435.htm> Accessed on 20 December 2016.

[12] Galeotti, M. "'Hybrid war' and 'little green men': How it works, and how it doesn't". *E-International Relations*, 16 April 2015. <http://www.e-ir.info/2015/04/16/hybrid-war-and-little-green-men-how-it-works-and-how-it-doesnt/> Accessed on 20 December 2016.

[13] Rettman, A." Nato chief warn Russia against 'green men' tactics". *EU Observer*. 18 August 2014. <https://euobserver.com/foreign/125281> Accessed on 20 December 2016.

[14] Kofman, M. & Rojansky, M. "A closer look at Russia's 'hybrid war". *KENNAN CABLE*, No. 7. <https://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf> Accessed on 20 December 2016, citing *The Military Doctrine of the Russian Federation* of 5 February 2010. <http://carnegieendowment.org/files/2010russia_military_doctrine.pdf > Accessed on 20 December 2016.

[15] Monaghan, A. "Putin's way of war: The 'war' in Russia's 'hybrid warfare'". *Parameters* 45(4). Winter 2015–16. 65.

[16] NATO, *op cit*, EN 12

[17] Johnson, R.F. "UPDATE: Russia's hybrid war in Ukraine 'is working'". *IHS Jane's Defence Weekly* 26. 2015.Original link no longer available, but see *Political Forum*, < http://www.politicalforum.com/warfare-military/399079-janes-russias-hybrid-war-ukraine-working.html > Accessed on 20 December 2016.

[18] Article 52 of AP I relates to the general protection of civilian objects and specifies that they shall not be the object of attack. 52§(3) provides that in case of doubt "whether an object which is normally dedicated to civilian purposes, such as a place of worship, a house or other dwelling or a school, is being used to make an effective contribution to military action, it shall be presumed not to be so used".

[19] "It won the 'intelligence war' to support combat operations. It even had successes in the 'information war' to undermine Western enthusiasm for direct involvement, at least until the tragic blunder which was the shooting down of MH17. However, the essence of 'non-linear war' is that all these diverse components must effectively combine to win the underlying 'political war' to achieve the desired aim, and here Moscow is losing, and losing badly." Galeotti, *op.cit*, EN 10.

[20] Bachmann, S-D. & Gunneriusson, H. “Russia’s hybrid warfare in the East: Using the information sphere as integral to hybrid warfare”. *Georgetown Journal of International Affairs* 2015. 198–212 and Bachmann, S-D. “Hybrid threats, cyber warfare and NATO’s comprehensive approach for countering 21st century threats – mapping the new frontier of global risk and security management”. 88 *Amicus Curiae* 2011.14-17.

[21] Fildes, J. "Stuxnet worm 'targeted high-value Iranian assets'", *BBC News.* 23 September 2010. < http://www.bbc.co.uk/news/technology-11388018>Accessed on 20 December 2016.

[22] Zetter, K. "An Unprecedented Look at Stuxnet, the World’s First Digital Weapon", *Wired*. 11 March 2013. <http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/> Accessed on 20 December 2016.

[23] A senior researcher for Kaspersky Lab, a leading computer security firm based in Moscow, Roel Schouwenberg, “spends his days (and many nights) ... battling the most insidious digital weapons ever, capable of crippling water supplies, power plants, banks, and the very infrastructure that once seemed invulnerable to attack”, see Kuschner, D. “The Real Story of Stuxnet”. *IEEE Spectrum.* 26 February 2013. <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet> Accessed on 22 December 2016.

[24] Liberatore, S. “Are autonomous robots the future of warfare? Experts warn of the dangers of using ‘smart’ weapons on the battlefield”. *Daily Mail.* 21 March 2016. <http://www.dailymail.co.uk/sciencetech/article-3503139/Are-autonomous-robots-future-warfare-Experts-warn-dangers-using-smart-weapons-battlefield.html> Accessed on 22 December 2016. See also Scharre, P. “Autonomous weapons fears and the Davos World Economic Forum”. *CNAS Press Note.* <https://www.cnas.org/press/press-note/cnas-press-note-autonomous-weapons-fears-and-the-davos-world-economic-forum> Accessed on 22 December 2016. For an interesting paper on the technique of ‘fuzzing’, which exploits software vulnerabilities, see Stephens, N. *et al*. “Driller: Augmenting fuzzing through selective symbolic execution”. <https://www.internetsociety.org/sites/default/files/blogs-media/driller-augmenting-fuzzing-through-selective-symbolic-execution.pdf> Accessed on 22 December 2016.

[25] Kofman, M. & Rojansky, M. *Op. cit*, EN 15.

[26] *Independent*. 26 February 2015. <http://www.independent.co.uk/news/world/europe/ukraine-crisis-putin-will-cut-gas-to-europe-unless-russia-is-paid-by-the-end-of-the-week-10071475.html > Accessed on 22 December 2016.

[27] Hazlehurst, J. “France famously blocked Pepsi’s purchase of yoghurt-maker Danone on national security grounds, and is often mocked for it. Jobs do not always fly overseas”. *Management Today.* 30 August 2012. <http://www.managementtoday.co.uk/features/1146256/buying-britain/> Accessed on 22 December 2016.

[28] Bird M & Pozzebon S. "Meet the Russian oligarchs who own the West's most famous brands" *Business Insider*. 5 February 2015. <http://uk.businessinsider.com/russian-oligarchs-that-own-western-companies-2015-2> Accessed on 22 December 2016.

[29] Critchlow, A. "Britain needs a new national oil company, not Russian oligarchs". *Daily Telegraph.* 6 March 2015. <http://www.telegraph.co.uk/finance/comment/11455849/Britain-needs-a-new-national-oil-company-not-Russian-oligarchs.html> Accessed on 22 December 2016.

[30] Glasgow, Aberdeen and Southampton airports were to become part of a consortium formed by Ferrovial, a Spanish transportation infrastructure firm which already has a 25% stake in HAH, and Macquarie – an Australia-based finance company. See Martin, S. "Heathrow Owner Sells Three British Airports to Foreign Buyers in £1bn Deal". *International Business Times.* 17 October 2014. <http://www.ibtimes.co.uk/heathrow-owner-sells-three-british-airports-foreign-buyers-1bn-deal-1470472>. Accessed on 22 December 2016.

[31] Brummer, A. "Britain for sale: How long before a foreign power turns out Britain's lights?" *Daily Mail.* 15 April 2012. <http://www.dailymail.co.uk/news/article-2130221/Britain-sale-How-long-foreign-power-turns-Britains-lights.html> Accessed on 22 December 2016.

[32] "Decision on new nuclear power plant 'delayed'". *BBC News.* 27 January 2016. <http://www.bbc.co.uk/news/business-35415187> Accessed on 22 December 2016.

[33] Yueh, L. "Britain for sale? " *BBC News.* 9 December 2013. <http://www.bbc.co.uk/news/business-25299230> Accessed on 22 December 2016.

[34] Grill, J. & Raupenstrauch, H. "Energiesicherheit Europas 2016". In Austrian Army (Österreichisches Bundesheer) *Sicher und Morgen? Sicherheits Politische Jahresvorschau 2016* (Security Political Preview for 2016), 146–148. op. cit. EN 8 Büro für Sicherheitspolitik.

[35] Klare, M.T. Europe's World. 21 March 2014. < http://europesworld.org/2014/03/21/europes-resource-dilemma-escaping-the-dependency-trap/#.Vq9JTtKLRpg > Accessed on 22 December 2016.

[36] FinanceScout24 "Atomausstieg: Deutschland verabschiedet sich von Kernenergie" , 5 December 2016 https://www.financescout24.de/wissen/ratgeber/atomausstieg; Die Welt " Energiewende - Bundestag beschliesst Atomausstieg bis 2022", 30 June 2011, <https://www.welt.de/politik/deutschland/article13460039/Bundestag-beschliesst-Atomausstieg-bis-2022.html> Accessed on 22 December 2016.

[37] "Interview: Lt. Gen. Ben Hodges", *Defense News.* 19 March 2015. < http://www.defensenews.com/story/defense/policy-

budget/leaders/interviews/2015/03/27/lt-gen-ben-hodges/70573420/ > Accessed on 22 December 2016.

[38] *Op. cit*, EN 15.

[39] The National Archive contains D3 Survey of Russian Espionage in the United Kingdom 1935–1955. See <http://discovery.nationalarchives.gov.uk/details/r/C11602765> Accessed on 22 December 2016.

[40] Kim Philby, Guy Burgess, Donald Maclean, Anthony Blunt and John Cairncross. Although a sixth member, Sir Roger Hollis, was suspected, nothing has been publicly substantiated. Despite his treachery, Anthony Blunt was knighted and appointed surveyor of the Queen's pictures and Director of the Courtauld Institute of Art. He was stripped of his knighthood when his treason became publicly known. See for a short account here: *BBC News* "The Cambridge spy ring" <http://news.bbc.co.uk/1/hi/special_report/1999/09/99/britain_betrayed/444058.stm> Accessed on 22 December 2016 and here: MI 5 Security Service <https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/sir-roger-hollis.html> Accessed on 22 December 2016.

[41] Mirror.Co.UK "What damage did Anthony Blunt's spy ring do to Britain?" *Daily Mirror*. 24 July 2009. <http://www.mirror.co.uk/news/uk-news/what-damage-did-anthony-blunts-spy-408455> Accessed on 22 December 2016. See also Boghardt, T. "The Cambridge Five, Spies with no regrets". *Spy Museum.* <https://www.spymuseum.org/education-programs/news-books-briefings/background-briefings/the-cambridge-five/>. Accessed on 22 December 2016.

[42] Wright, P. & Greengrass, P. *Spycatcher: The candid autobiography of a senior intelligence officer.*New York, Viking Press, 1987, 2.

[43] Buchanan, RT. "Russian military aircraft spotted in British skies near Nato monitoring base". *Independent.* 20 May 2015. <http://www.independent.co.uk/news/uk/home-news/russian-military-aircraft-spotted-in-british-skies-near-nato-monitoring-base-10264388.html> Accessed on 22 December 2016.

[44] Whitehead, T. "Number of Russian Spies in the UK back to Cold War levels, say security services" *The Telegraph*. 6 April 2012. <http://www.telegraph.co.uk/news/uknews/defence/9190536/Number-of-Russian-spies-in-the-UK-back-to-Cold-War-levels-say-security-services.html> Accessed on 22 December 2016. See also Gordievsky. O. "Russia has as many spies in Britain now as the USSR ever did". *Guardian.* 11 March 2013. <http://www.theguardian.com/world/2013/mar/11/russian-spies-britain-oleg-gordievsky>. Accessed on 22 December 2016

[45] For example: Terrorism Act 2000; Anti-terrorism, Crime and Security Act 2001; Terrorism Act 2006; Counter-Terrorism Act 2008; Terrorism Prevention and Investigation Measures Act 2011; Counter-Terrorism and Security Act 2015.

[46] Adopted by the State Duma on 8 December 1995, signed by Russian Federation President B Yeltsin on 10 January 1996. <http://fas.org/irp/world/russia/docs/law_960110.htm> Accessed on 22 December 2016.

[47] Lilleker, DG. *Against the Cold War: The history and political traditions of pro-Sovietism in the British Labour Party, 1945–89*. London: I.B.Tauris, 2004, 91.

[48] Former SVR officer Alexander Kouzminov, the author of *Biological espionage*, which provides "an inside account of his work within the top secret 'Directorate S' where he helped implement Russia's plans for biological espionage and biological warfare". See his interview, Comstock, P. "False Flags, Ethnic Bombs and Day X". *California Literary Review*, 31 March 2007. <http://calitreview.com/62/false-flags-ethnic-bombs-and-day-x/> Accessed on 22 December 2016.

[49] Mitrokhin,V. & Andrew, C. *The Mitrokhin Archive*: *The KGB in Europe and the West*. Penguin Books Ltd, 2000.

[50] Culbertson, A. "Europe on 'BRINK OF WAR' as Turkey gathers boats to ship migrants to Greece over EU anger". *Daily Express.* 30 November 2016. <http://www.express.co.uk/news/world/737480/Europe-war-Turkey-migrants-Greece-EU-Erdogan> Accessed on 22 December 2016.

[51] See Bachmann, op.cit EN 4.

[52] <http://www.legislation.gov.uk/ukpga/1998/42/contents> Accessed on 22 December 2016.

[53] *Council of Europe*: <http://www.echr.coe.int/Documents/Convention_ENG.pdf> Accessed on 22 December 2016.

[54] UN Refugee Agency: <http://www.unhcr.org/3b66c2aa10.html> UK Signature: 1951, Ratification/UK Accession: 1954: < http://treaties.fco.gov.uk/docs/pdf/1954/TS0039.pdf > Accessed on 22 December 2016.

[55] UN Office of the High Commissioner: <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx> UK Signature: 1966, UK Ratification/Accession: 1976: < http://treaties.fco.gov.uk/docs/pdf/1977/TS0006.pdf > Accessed on 22 December 2016.

[56] UNCAT. December 1984. <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CAT.aspx> UK Signature: 1985, Ratification/Accession: 1988, enacted 1989, < http://treaties.fco.gov.uk/docs/pdf/1991/TS0107.pdf > Accessed on 22 December 2016.

[57] Convention on the Rights of the Child. < http://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx> Accessed on 22 December 2016. UK Signature: 1990. Ratification/Accession: 1992; see Article 10.1 "In accordance with the obligation of States Parties under

article 9, paragraph 1, applications by a child or his or her parents to enter or leave a State Party for the purpose of family reunification shall be dealt with by States Parties in a positive, humane and expeditious manner. States Parties shall further ensure that the submission of such a request shall entail no adverse consequences for the applicants and for the members of their family".

[58] Optional Protocol to the Convention on the Rights of the Child on the involvement
of children in armed conflict.
<http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPACCRC.aspx> Accessed on 22 December 2016. Accessed on 22 December 2016.

[59] *Op. cit*, Bachmann.

[60] Faiola, A. & Mekhennet, S. "Tracing the path of four terrorists sent to Europe by the Islamic State". *The Washington Post.* 22 April 2016. <https://www.washingtonpost.com/world/national-security/how-europes-migrant-crisis-became-an-opportunity-for-isis/2016/04/21/ec8a7231-062d-4185-bb27-cc7295d35415_story.html?utm_term=.440eefaf21c1> Accessed on 22 December 2016. See also Simcox, R. "The threat of Islamist terrorism in Europe and how the US should respond". *The Heritage Foundation.* 1 August 2016: "The director of Europol recently described the current situation as 'the highest terrorist threat we have faced for over 10 years'. These security concerns are being exacerbated by unprecedented levels of migration into Europe from impoverished and/or war-torn areas of the Middle East, Africa, and the Balkans, with ISIS known to have targeted such routes for infiltration". <
http://www.heritage.org/research/reports/2016/08/the-threat-of-islamist-terrorism-in-europe-and-how-the-us-should-respond > Accessed on 22 December 2016.

[61] Spencer, R.: *Stealth Jihad: How radical Islam is subverting America without guns or bombs hardcover*. Regnery Publishing; First Edition (October 28, 2008); see also by the same author, "The Hijrah into Europe, refugees" colonize a continent". *Frontpage Magazine.* 4 September 2015. <http://www.frontpagemag.com/fpm/260019/hijrah-europe-robert-spencer> Accessed on 22 December 2016. Hohmann, L.: "ISIS smuggler: 'We will use refugee crisis to infiltrate West'", *InfoWars*. 5 September 2015. <http://www.infowars.com/isis-smuggler-we-will-use-refugee-crisis-to-infiltrate-west/> Accessed on 22 December 2016. Also Brown, A., "Just wait … Islamic State reveals it has smuggled THOUSANDS of extremists into Europe", *Daily Express.* 18 November 2015. <http://www.express.co.uk/news/world/555434/Islamic-State-ISIS-Smuggler-THOUSANDS-Extremists-into-Europe-Refugees > Accessed on 22 December 2016.

[62] Blair, O., "ISIS jihadists 'infiltrating' Europe through refugee crisis". *Independent.* 14 September 2015.

<http://www.independent.co.uk/news/world/europe/pope-francis-fears-isis-jihadists-infiltrating-europe-through-refugee-crisis-10499969.html> Accessed on 22 December 2016. For anecdotal accounts see by Noble, S."ISIS Fighters Use Refugee Crisis to Infiltrate the EU" *Independent Sentinel*. 6 September 2015,<http://www.independentsentinel.com/isis-fighters-use-refugee-crisis-to-infiltrate-the-eu/> Accessed on 22 December 2016.

[63] Coughlin, C. "Isil is taking advantage of the EU's incompetence". *Daily Telegraph.* 26 January 2016. <http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/12123720/Isil-is-taking-advantage-of-the-EUs-incompetence.html. Accessed on 22 December 2016.

[64] *Ibid*.

[65] "Public services and infrastructure | Key topics". *Migration Watch.* November 2016 <https://www.migrationwatchuk.org/key-topics/public-services-infrastructure> Accessed on 22 December 2016.

[66] Green, A. "At last, the truth about immigration and council house queue jumping". *Migration Watch.* 30 June 2009. <https://www.migrationwatchuk.org/press-article/64> Accessed on 22 December 2016.

[67] "Germany shocked by Cologne New Year gang assaults on women". *BBC News.* 5 January 2016. <http://www.bbc.com/news/world-europe-35231046> Accessed on 22 December 2016.; "'Cultural differences' led to migrant sexually assaulting child at UK train station". *Daily Express.* 6 March 2016. <http://www.express.co.uk/news/uk/650257/Cultural-differences-somalian-migrant-sexually-assaulting-child-UK-train-station> Accessed on 22 December 2016.Hall, A. "Group of migrants accused of sexually assaulting 18 women at Germany concert". *Daily Mirror.* 31 May 2016. <http://www.mirror.co.uk/news/world-news/group-migrants-accused-sexually-assaulting-8087347> Accessed on 22 December 2016; Osborne, S."Iraqi refugee 'raped 10-year-old boy at Austrian swimming pool'". *Independent*. 6 February 2016. <http://www.independent.co.uk/news/world/europe/iraqi-refugee-raped-10-year-old-boy-at-austrian-swimming-pool-a6857721.html> Accessed on 22 December 2016.

[68] Euractive: <http://www.euractiv.com/sections/global-europe/eu-mulls-plan-take-charge-europes-borders-320152> Accessed on 22 December 2016.

[69] Troianovski, A. & Thomas, A. "Germany Imposes Border Checks Amid Migrant Wave" *Wall Street Journal*. 13 September 2015. <http://www.wsj.com/articles/germany-needs-help-to-deal-with-migrant-crisis-cabinet-minister-says-1442155684> Accessed on 22 December 2016.

[70] News Wires "'Schengen zone on the brink' as EU edges closer to suspending open borders" *France 24* 25 January 2016

<http://www.france24.com/en/20160125-european-union-edges-closer-suspending-schengen-zone-open-borders> Accessed on 22 December 2016.

[71] Soros, G. "Refugee crisis: Putin's Russia in race with EU to see which will collapse first". *Irish Examiner*. 11 February 2016. <http://www.irishexaminer.com/viewpoints/analysis/refugee-crisis-putins-russia-in-race-with-eu-to-see-which-will-collapse-first-381172.html> Accessed on 22 December 2016.

[72] Mosquera, A. & Bachmann, S-D., *op. cit.*, p. 4.

[73] Dunlap, C. "Lawfare today: A perspective". *Yale Journal of International Affairs* Winter 2008. 146.

[74] European External Action Service. "Food-for-thought paper 'Countering Hybrid Threats'". 13 May 2015. <http://www.statewatch.org/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf> Accessed on 22 December 2016.

[75] On US intelligence sharing in the Syrian war, see Hersh, SM. "Military to Military". *London Review of Books*, Vol. 38 No. 1 · 7 January 2016, pages 11-14: <http://www.lrb.co.uk/v38/n01/seymour-m-hersh/military-to-military > Accessed on 22 December 2016.

[76] Cost of Baha Mousa Inquiry £13 544 761; see The National Archives, "The Baha Mousa Public Inquiry" .31 October 2011. <http://webarchive.nationalarchives.gov.uk/20120215203912/http://www.bahamousainquiry.org/costs/index.htm> Accessed on 22 December 2016.

The costs of Al Sweady Inquiry: £24 901 050; see The National Archives."Al-Sweady Public Inquiry", 31 December 2014. <http://webarchive.nationalarchives.gov.uk/20150115114702/http:/www.alsweadyinquiry.org/costs/index.htm> Accessed on 22 December 2016.; The Iraq Inquiry (financial year 2014 to 2015): £10 375 000; see The Iraq Inquiry. "Iraq Inquiry costs for the financial year 2016 to 2017". 2 November 2016. < http://www.iraqinquiry.org.uk/the-inquiry/news-archive/2016/2016-11-02-2016-17-costs/ > Accessed on 22 December 2016.; "The MOD Annual Report and Accounts also reveals that the provision for legal claims has been increased annually, standing currently at £130 million" in Tugendhat, T. & Croft, L., "The Fog of Law-An Introduction to the legal erosion of British Fighting Power", *Policy Exchange*, 2013, p35 < https://policyexchange.org.uk/publication/the-fog-of-law-an-introduction-to-the-legal-erosion-of-british-fighting-power/ > Accessed on 22 December 2016.

[77] *Ibid*, discussing the "legal erosion of British fighting power"

[78] SM is an Afghan national who was captured and detained by UK armed forces on 7 April 2010 in Afghanistan during the course of a 10-hour long planned military operation, during which three British servicemen were wounded and SM's co-fighter was killed. He was transferred into Afghan custody on 25 July 2010 and subsequently convicted in the Afghan courts of offences relating to the insurgency in Afghanistan. He was released from prison in

June 2014. SM brought claims for damages under the HRA alleging breaches of articles 3, 5, 6 and 8 ECHR. He has also brought tort claims under Afghan law equivalent to assault, battery, false imprisonment, misfeasance in public office and negligence. The courts below ruled on a number of preliminary issues relating to the claims for deprivation of liberty, holding that the claims were not precluded by the doctrine of Crown act of state, that the respondent's detention after 96 hours was contrary to Article 5 ECHR and s. 6 of the Human Rights Act 1998, and that the respondent's detention after 72 hours was unlawful under Afghan law. Mohammed and others (Respondents) v Ministry of Defence (Appellant) [2016] Supreme Court, Case ID: UKSC 2015/0218. The case presents a legal 'Catch 22', in that handing Mohammed over to the Afghan authorities would have given rise to a claim under Article 3 (the risk of torture or to inhuman or degrading treatment or punishment), while retaining him breached Article 5 (the right to liberty and security) and releasing him would have posed a serious threat to the safety of the force.

[79] General Sir Nick Carter warned that legal claims made against the military could undermine Britain's ability to fight future wars. He "warned that the threat of legal action would make soldiers afraid of making 'honest mistakes' in war zones": Coughlin, C. "Legal action against soldiers 'could undermine Britain on the battlefield' warns chief of general staff", *Daily Telegraph.* 29 January 2016. <http://www.telegraph.co.uk/news/uknews/defence/12130929/Legal-action-against-soldiers-could-undermine-Britain-on-the-battlefield-warns-chief-of-general-staff.html> Accessed on 22 December 2016.

[80] [2010] EWCA Civ 65, CA.

[81] *Op. cit*., Clearing the Fog of Law, 2015, *Policy Exchange*, at 9.

[82] *Op.cit*, Food-for-thought paper "Countering Hybrid Threats".

[83] See *supra*.

[84] One of the lawyers who has been at the forefront of representing Iraqis who were allegedly victims of abuse by British servicemen is now under investigation himself for the firm's activities in mounting claims against UK service personnel over alleged atrocities in Iraq and faces a professional disciplinary hearing. The firm, Public Interest Lawyers, ceased to act for 187 Iraqi claimants because of its 'permanent closure'. At the beginning of August 2016, the Legal Aid Agency announced it had terminated its contract with Public Interest Lawyers, saying the firm had breached contractual requirements. Gross, M. "Public Interest Lawyers to close". *The Law Society Gazette.* 15 August 2016. <https://www.lawgazette.co.uk/news/public-interest-lawyers-to-close/5057124.article>. Accessed on 27 December 2016. The firm's problems arose out of the findings of the Al Sweady Inquiry, that witness claimed the victims were taken prisoner by British soldiers, and later mistreated and murdered. But the Public Inquiry eventually found there was no concrete evidence the insurgents had been unlawfully killed while

prisoners of the British Army. See Mullen, E. "Public Interest Lawyers defend £22m inquiry into Iraq deaths". *Birmingham Post.* 28 March 2014. <http://www.birminghampost.co.uk/business/legal/public-interest-lawyers-defend-22m-6886761> Accessed on 27 December 2016. The report for the Al Sweady Inquiry is available from <https://www.gov.uk/government/publications/al-sweady-inquiry-report> Accessed on 27 December 2016.

[85] The North Atlantic Treaty, Article 5 states that "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."

[86] "Case concerning military and paramilitary activities in and against Nicaragua". See §187 *et seq* of Judgment (Merits) of 27 June 1986. <http://www.icj-cij.org/docket/files/70/6503.pdf> Accessed on 27 December 2016.

[87] A/RES/29/3314, Art. 3(b). < http://www.un-documents.net/a29r3314.htm

[88] Rome Statute of the International Criminal Court, https://www.icc-cpi.int/nr/rdonlyres/ea9aeff7-5752-4f84-be94-0a655eb30e16/0/rome_statute_english.pdf> Accessed on 27 December 2016. The conditions for entry into force of the crime of aggression decided upon in Kampala provide that the Court will not be able to exercise its jurisdiction over the crime until after 1 January 2017 when a decision is to made by state parties to activate the jurisdiction. <http://www.iccnow.org/?mod=aggression>. Accessed on 27 December 2016.

[89] A/RES/29/3314, *op. cit.* Art. 3(b). See also *Handbook ratification and implementation of the Kampala amendments to the Rome Statute of the ICC – Crime of aggression war crimes.* < http://dataspace.princeton.edu/jspui/bitstream/88435/dsp012b88qc227/1/LISD_ICC2012.pdf > Accessed on 27 December 2016.

[90] Art 2 (4) UN Charter reads, "All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations."

[91] "Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of

any state or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter Vll."

[92] Art 51 UN Charter reads "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."

[93] ICRC. "Rule 14. Proportionality in Attack", *Customary IHL*. <: https://www.icrc.org/customary-ihl/eng/docs/v1_cha_chapter4_rule14>. Accessed on 27 December 2016.

[94] Roscini, M. *Cyber operations and the use of force in international law*. Oxford: OUP, 2014 .

[95] Norton anti-virus says about this virus: "It is sophisticated, well-funded, and there are not many groups that could pull this kind of threat off. It is also the first cyberattack we've seen specifically targeting industrial control systems". Norton. "The STuxnet Worm"<http://uk.norton.com/stuxnet/>. Accessed on 27 December 2016.

[96] *Tallinn 2.0*, the follow-on project to the *Tallinn Manual on the International Law Applicable to Cyber Warfare*. The focus of the original Tallinn Manual is on the most disruptive and destructive cyber operations – those that qualify as 'armed attacks' and therefore allow states to respond in self-defence, and those taking place during armed conflict. Schmitt, M. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* CUP. 2013.

[97] See Articles on responsibility of states for internationally wrongful acts, Resolution A/RES/56/83, adopted by the General Assembly on 28 January 2002. <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/56/83>. Accessed on 27 December 2016. Its Article 4 states, "1. The conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central government or of a territorial unit of the State. 2. An organ includes any person or entity which has that status in accordance with the internal law of the State".

[98] *Ibid.*, article 8.

[99] *Responsibility of States for Internationally Wrongful Acts 2001*, art. 4(2): "An organ includes any person or entity which has that status in accordance with the internal law of the State". States will also be responsible for the conduct of "a person or entity which is not an organ of the State under article 4 but

which is empowered by the law of that State to exercise elements of the governmental authority", *ibid.,* art 5, Articles on Responsibility of States for Internationally Wrongful Acts 2001.

[100]Norton-Taylor, R. "UK's nuclear deterrent entirely dependent on the US – crossparty report". *The Guardian.* 1 July 2014: "Not only are Britain's Trident missiles in a common pool shared with the US and maintained in Kings Bay, Georgia, its nuclear warheads are designed and maintained at the Atomic Weapons Establishment at Aldermaston with the help of US know-how, as recently declassified documents on the UK-US Mutual Defence Agreement confirmed". <https://www.theguardian.com/uk-news/defence-and-security-blog/2014/jul/01/trident-nuclear-weapons-uk>. Accessed on 27 December 2016. The Agreement between UK and US, for Co-operation on the Uses of Atomic Energy for Mutual Defence Purposes, 1958, is a bi-lateral mutual security and defence agreement and is available at <http://treaties.fco.gov.uk/docs/pdf/1958/TS0041.pdf> Accessed on 27 December 2016. See also "Exclusive: UK to step up collaboration with US over nuclear warheads – documents released under FoI reveal 'enhanced collaboration' plans, raising questions over independence of UK deterrent". *Guardian.* 12 June 2014. <https://www.theguardian.com/world/2014/jun/12/uk-us-mutual-defence-agreement-exclusive> Accessed on 27 December 2016.

[101] *Ibid.*, art. 6

[102] Crawford, J. "Articles on Responsibility of States for Internationally Wrongful Acts 2001, Historical background and development of codification". UN Audiovisual Library of International Law < http://legal.un.org/avl/ha/rsiwa/rsiwa.html> Accessed on 27 December 2016.

[103] See also supra, at EN 27, and "Second Chinese company poised to invest in Hinkley Point". *The Telegraph.* 7 May 2016. <http://www.telegraph.co.uk/business/2016/05/07/second-chinese-company-poised-to-invest-in-hinkley-point/> Accessed on 27 December 2016.

[104] Islamic State (IS) is a movement that is regarded as a serious threat to Russia's security. See "Russia keeps eye on Islamic State". *Al Monitor.* 21 August 2014. < http://www.al-monitor.com/pulse/originals/2014/08/russia-iraq-monitor-situation.html> Accessed on 27 December 2016. See also "Islamic State threat to Russia is real – FSB". *RT.* 10 April 2015. <https://www.rt.com/politics/248685-russia-islamic-state-threat/> Accessed on 27 December 2016.

[105] *Cf* European Council on Foreign Relations, "Russian intervention in Syria" http://www.ecfr.eu/debate/syria_russia_vfc. Accessed on 27 December 2016. Kashin, O. "Russia's intervention in Syria could have been stopped 20 years ago", *The Guardian,* 2 November 2016. https://www.theguardian.com/world/2016/nov/02/russia-intervention-syria-stopped-20-years-ago-chechnya-war> Accessed on 27 December 2016.

[106] Simon, S. & Stevenson,J. " Don't intervene in Syria". *New York Times.* 6 October 2016. <http://www.nytimes.com/2016/10/06/opinion/dont-intervene-in-syria.html>. Accessed on 27 December 2016.

[107] Reflexive control is the term used by Russia for information warfare. See Snegovay,M. *Putin's information warfare in Ukraine: Soviet origins of Russia's hybrid warfare.* Institute for the Study of War, 2015. <http://understandingwar.org/sites/default/files/Russian%20Report%201%20Putin's%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf>. Accessed on 27 December 2016.

[108] *Op.cit.* Galeotti, M. *"'Hybrid war' and 'little green men': How it works, and how it doesn't"*.

[109] *Op. cit.* Gerasimov, V. *The value of science in prediction*.

[110] *Ibid*.

[111] Iskander can be fitted with either nuclear or conventional warheads, have a range of up to about 300 miles, putting much of Poland in reach. Press Association. "US to activate European missile defence system in Romania and Poland". *Evening Express.* 11 May 2016. <https://www.eveningexpress.co.uk/pipe/news/international/us-to-activate-european-missile-defence-system-in-romania-and-poland/>. Accessed on 27 December 2016

[112] The concern over reductions in defence spending by European NATO nations as a means to reduce debt and government expenditures caused consternation in the US. Michaels, M. "Crisis-stricken NATO members downsize armed forces, raising eyebrows in Washington". *Mint Press.* 19 June 2013. <http://www.mintpressnews.com/crisis-stricken-nato-members-downsize-armed-forces-raising-eyebrows-in-washington/163871/>. Accessed on 27 December 2016.

[113] Lord Richards of Herstmonceux, when Chief of the Defence Staff, made some withering remarks about Prime Minister David Cameron's approach to dealing with ISIS in Syria.The former army chief is also quoted as telling Mr Cameron that being a cadet at Eton did not qualify him to decide tactics. See Wintour, P. & Quinn, B."Lord Ashcroft biography claims David Cameron faced military criticism". *The Guardian.* 22 September 2015. <https://www.theguardian.com/politics/2015/sep/22/lord-ashcroft-biography-david-cameron-defence-book-syria-libya>. Accessed on 27 December 2016.