HYBRID WARS: THE 21 CENTURYS NEW THREATS TO GLOBAL PEACE AND SECURITY

SaschaDominik Bachmann, Bournemouth University, Gunneriusson Swedish Defence University

This article discusses a new form of war, hybrid war, with inclusion of aspects of cyberterrorism and cyberwar against the backdrop of Russias Ukrainian Spring and the continuing threat posed by radical Islamist groups in Africa and the Middle East. It also discusses the findings of an ongoing hybrid threat project by the Swedish Defence College. This interdisciplinary article predicts that military doctrines, traditional approaches to war and peace and their perceptions will have to change in the future.

Introduction

The socalled Jasmine Revolution during the Arab Spring of 2011 challenged the political order in the Maghreb and the whole Middle East. While

some of the protests led to actual regime changes and a move towards freedom and democracy such as in Tunisia events in other states in the region, such as Bahrain and Syria, had been less successful and saw the

a Assessor Jur, LLM (Stel) LLD (UJ), Associate Professor in International Law (Bournemouth University, UK). Outside academics, he has served in various capacities as lieutenant colonel (army reserve), taking part in peacekeeping missions in operational and advisory capacities The author took part as NATOs Rule of Law Subject Matter Expert (SME) in NATOs Hybrid Threat Experiment of 2011 and in related workshops at NATO and national level.

b PhD in Modern History, Associate Professor in War Studies, head of research ground operative and tactical areas Department of Military Studies, War Studies Division, Land Operations Section, Swedish Defence University.

return of the old order of autocratic governments. The collapse of Muammar Gaddafis regime in Libya, the ongoing civil unrest in Egypt between supporters of the ousted hardline Muslim brotherhood and the military government, the ongoing brutal Syrian conflict and the collapse of Iraq after the withdrawal of the USA have all significantly contributed to the proliferation and the ascent of evermore powerful and murderous terrorist groups and organisations across the region.

The use of cyber1 and kinetic responses to international terrorism have increasingly blurred the traditional distinction between war and peace. Such a distinction was replaced by the recognition of a notion of new, multimodal threats, which have little in common with past examples of interstate aggression. These new threats to global peace and security seriously threaten our modern Western way of life within the context of the present steadystate environment at home (and against the backdrop of the ongoing asymmetric conflicts in Afghanistan, Pakistan, Mali, Somalia, Kenya and Yemen). These new wars along asymmetric lines of conflict2 constitute a dichotomous choice between counterinsurgency and conventional war3 and challenge traditional concepts of war and peace.

This article4 firstly reflects on the new notion of socalled hybrid threats as a rather new threat definition and its (temporary) inclusion in the North Atlantic Treaty Organizations (NATO) new comprehensive defence approach with a reflection on the last Swedish experiment. Secondly, it discusses the use of cyber in the context of hybrid threats before it, thirdly, addresses some implications for military doctrine arising from such threats. The article concludes with a brief outlook on new dimensions of possible future threats to peace and security by highlighting the evolvement of the concept of hybrid threats into hybrid war by reflecting on security issues arising.

Hybrid threats as challenges to peace and security

The novel concept of hybrid threats first gained recognition when Hezbollah had some tangible military success against the Israeli Defense Forces (IDF) in Lebanon 2006 during the Second Lebanon War.5 Ironically, the definition of hybrid then was that a nonstate actor showed military capabilities one originally only associated with state actors.6 Multimodal, lowintensity, kinetic as well as non kinetic threats to international peace and security include cyber war, asymmetric conflict scenarios, global terrorism, piracy, transnational organised crime, demographic challenges, resources security, retrenchment from globalisation and the proliferation of weapons of mass destruction. Such (multi)modal threats have become known as hybrid threats.7 Recognised in NATOs BiStrategic Command

Capstone Concept of 2010, hybrid threats are defined as those posed by adversaries, with the ability to simultaneously employ conventional and non conventional means adaptively in pursuit of their objectives.8 Having identified these threats, NATO undertook work on a comprehensive conceptual framework, as a Capstone Concept, which was to provide a legal framework for identifying and categorising such threats within the wider frame of possible multistakeholder responses. In 2011, NATOs Allied Command Transformation (ACT), supported by the US Joint Forces Command Joint Irregular Warfare Centre (USJFCOM JIWC) and the US National Defence University (NDU), conducted specialised workshops related to Assessing Emerging Security Challenges in the Globalised Environment (Countering Hybrid Threats [CHT]) Experiment.9 These workshops took place in Brussels (Belgium) and Tallinn (Estonia) and were aimed at identifying possible threats and at discussing some key implications when countering such risks and challenges. In essence, hybrid threats faced by NATO and its nonmilitary partners require a comprehensive approach allowing a wide spectrum of responses, kinetic and nonkinetic, by military and nonmilitary actors. In a 2011 report, NATO describes such threats as,

Admittedly, hybrid threat is an umbrella term, encompassing a wide variety of existing adverse circumstances and actions, such as terrorism, migration, piracy, corruption, ethnic conflict etc. What is new, however, is the possibility of NATO facing the adaptive and systematic use of such means singularly and in combination by adversaries in pursuit of longterm political objectives, as opposed to their more random occurrence, driven by coincidental factors.10

The same report underlines that hybrid threats are not exclusively a tool of asymmetric or nonstate actors, but can be applied by state and nonstate actors alike. Their principal attraction from the point of view of a state actor is that they can be largely nonattributable, and therefore applied in situations where more overt action is ruled out for any number of reasons.

The findings of the two workshops were published in the ACTs final report and recommendations in 2011. However, due to a lack of financial resources in general and an absence of the political will to create the necessary smart defence capabilities among its member states, NATO decided in June 2012 to cease work on CHT at its organisational level while encouraging its member states and associated NATO Excellence Centres to continue working on hybrid threats.

In 2012, the Swedish National Defence College as a Partnership for Peace (PfP) partner11 conducted its own hybrid threat experiment.12 The scenario dealt with a fictitious adversary in the East, not very dissimilar to Belorussia, except that it was an island kingdom in the Baltic Sea. The situation deteriorated to the point where neighbouring states were directly affected by a mix of conventional military and hybrid threats. More traditional threats arose from the attempt to sink a hijacked oil tanker in the middle of the sensitive maritime environment zone, launching a small group of Special Forces operatives (SFOs) in Swedish territory and hiring Somali pirates to hijack Swedish vessels off the Horn of Africa. The latter showed how a conflict could spread from being very local in one part of the world to involve remote hotspots in Africa. In this case, the problems at the Horn of Africa could legitimise actions and events, which originally had their roots in Northern Europe. The participants of the experiment acted as a committee of advisers for the Swedish government, and their individual roles represented their normal functions: from members of the armed forces and national support agencies to the university sphere, the pharmacological industry, banking and internet security. The experiment showed that existing and established standard operation procedures (SOPs) made responding to specific threats rather efficient. This was mostly due to already established command and control as well as communication and coordination assets and abilities. The experiment did however also show the existence of shortcomings when countering multimodal threats due to the absence of a nationally defined comprehensive approach for a joint interagency approach. With SOPs in place and lacking a uniform command and control structure, it can also become harder to respond in a tailored and united way for government agencies, as all contributing agencies have their respective tasks and procedures. This lack of comprehensive joint action and coordination is highlighted by the fact that the government in the scenario did not have the authority to direct and control the work of subordinate but autonomous agencies.13 The participants of the hybrid threat experiment did recognise that a coming hybrid conflict would lead to new levels of threat and response complexity and that there was a need for active, uniform and collective leadership beyond SOPs.14 The participants identified as a weakness the lack of a comprehensive response and coordination between agencies such as the armed forces, the civil defence assets and other civilian actors, such as IT specialists and pharmaceutical experts.15 With a shrinking defence budget, the downscaling of agencies and an obvious lack of civil society to accept the potential existence of such threat in the future, it seems unlikely that these shortcomings will be addressed in the near future.

In an African and Middle Eastern context, one cannot generalise as these states differ in terms of stability and strength regarding the capacities of their security assets. A state such as South Africa should and could rely very much on SOPs in order to have a constant high readiness against unsuspected threats. Other countries with weaker infrastructures and resources cannot expect their agencies to react swiftly when faced with ad hoc security challenges. The recommendation should then be to have very able actors (rather than structures, which the SOP demands) at key positions (at ministerial level and the level below) who can understand the threat and swiftly tailor a suitable response with the resources the state has at hand itself and with allied states. The latter is important in general and certainly so in Africa. As the borders have a colonial past, one should expect hybrid threats stemming from nonstate actors (NSAs), which will eventually encompass a number of states.

Worrying and of particular relevance in the context of hybrid threats is the danger of proliferation of advanced weapon systems by NSAs associated with radical Islam, as for example the Islamic State of Iraq and alSham (ISIS) in Syria and Iraq as well as the increasing use of new technologies by NSAs. The last Israel Gaza conflict highlights these developments: new technologically advanced rocket systems, supplied by Iran to their terrorist proxy Hamas, were used against Israel. The capability of the Fajr (Dawn) 5 rocket to reach both Tel Aviv and Jerusalem has been shown and has once more shown the vulnerability of Israel as a state when it comes to conventional, kinetic threats.

Against the backdrop of the ongoing conflict in Ukraine and the classification of the conflict as a hybrid war by Ukraines national security chief,16 NATOs decision to discontinue working on the hybrid concept as an organisational.