Center for Security Studies

STRATEGIC TRENDS 2015

Key Developments in Global Affairs

STRATEGIC
TRENDS 2015

Key Developments in Global Affairs

Editors: Oliver Thränert, Martin Zapfe

Series Editor: Andreas Wenger

Authors: Myriam Dunn Cavelty, Jonas Grätz, Michael Haas,
                   Prem Mahadevan, Martin Zapfe

CSS
ETH Zurich

ETH *zürich*

Contents

Acknowledgments

Strategic Trends 2015: Introduction

While introducing last year's volume of *Strategic Trends*, we diagnosed that '*beyond a mere decline of Western influence, the chapters of this volume reflect a basic insecurity over the future direction of these geopolitical shifts.*' One year on, and, while editing *Strategic Trends 2015*, we could not help but conclude that this basic insecurity not only continued, but deepened.

As is tradition in the Strategic Trends series, the CSS staff debated which developments would shape international politics in the coming year and beyond. As a result stand five chapters that are consciously unrelated and are each identified for their own reasons. The chapters introduce and analyze key trends in international affairs – without claiming to have covered every important development in world politics.

Two themes are interwoven in every one of the chapters, in varying degrees and characters: *Norms* and *order*. The systemic challenge that Putin's Russia poses to a liberal EU, described by **Jonas Grätz**, is one of norms and values. Putin's propagated revival of orthodoxy and nationalism coupled with his call for 'new rules' in the international order on the European continent challenges not just this order but the very basis of the EU's homogeneity. The Middle East, the other crisis-ridden region of 2014, seems to be on the verge of a long struggle for a re-establishment, or re-invention, of regional and intra-state order, says **Martin Zapfe**. The effects of this struggle, and of competing concepts of the state and concepts of ruling within the Middle East, writes **Prem Mahadevan**, touch Europe directly – not least through a new 'territorial terrorism' embodied by IS. Beyond those two geographical regions, two other chapters describe spaces where norms may just be emerging. Space, covered by **Michael Haas**, and Cyberspace, analyzed by **Myriam Dunn Cavelty**, represent global commons that will further move to the forefront of international affairs – and with them the question of which norms, if any, should guide those affairs.

Thus, the diagnosed basic insecurity over the future of international affairs deepens, as it evolves from changes within the balance of power to the questioning of the very system in which state power is generated and applied. While far from being an exclusively pessimistic diagnosis, it seems that the doubts the 'West' holds over the universality of its values contributes to the general insecurity of these times.

As in previous editions of the *Strategic Trends* series, the chapters refrain from giving policy recommendations, although the analytical standpoint of each author might become clear. We do wish you an enriching read and hope that *Strategic Trends 2015* might succeed in stimulating debates and provoking arguments – to overcome the basic insecurity of today, these debates are in dire need.

The Middle East's Thirty Years' War?

Martin Zapfe

> The Middle East seems to be on the verge of a 'New Thirty Years' War' that is characterized by a disintegrating regional order, a contest between secular and religious concepts of domestic and regional politics, and the potential for new and unlikely alliances. What is at stake in 2015 and beyond, in short, is not only the future of the states in the region, but the concept of statehood in the Arab world per se.

Displaced people from the minority Yazidi sect, fleeing violence from the 'Islamic State' in Sinjar town, walk towards the Syrian border near the Syrian border town of Elierbeh, 10 August 2014.

A most modern form of war

Few reports on the states between Egypt in the West and Iran in the East written during the past decades would have spoken of systemic stability and benevolent conditions for the region. Nevertheless, 2014 was an especially difficult year, having seen the biggest challenge to the regional order since the Iranian Revolution of 1979. At the center stands the Syrian carnage; a revolt-turned-civil-war-turned-proxy war in a country that for decades was party to many conflicts, yet whose internal stability was mostly taken for granted. After more than three years, immeasurable suffering, and over 200,000 deaths, the conflict has now openly spilled over the border into Iraq (again).

With the advent of the so-called 'Islamic State' (IS), for the first time in decades, a single party combines the necessary ideological zeal, determination, and military skill to implement a revisionist agenda and redraw regional borders – or, more precisely, to erase them altogether in an effort to shake off the very concept of the state as an unwanted colonial heritage. The future of the IS appears in no way clear; in fact, at the time of writing, a sudden collapse in large parts of the territory where it is openly operating seems to be a real possibility. However, its mere presence and success is no coincidence, but just the most prominent sign of currents challenging the region's order.

As numerous observers have noted, the Middle East seems to be on the verge of a conflict that can, with good reasons, be described as a 'New Thirty Years' War'. This is also the core of this chapter's key argument: The region is threatening to slide into a conflict that is characterized by a disintegrating regional order, a contest between secular and religious concepts of domestic and regional politics, the potential for new and unlikely alliances, and all that within a disintegrating center. What is at stake in 2015 and beyond, in short, is not only the future of the states in the region, but the concept of statehood in the Arab world per se.

To bring forward this argument, and to highlight possible implications, the chapter proceeds in two steps: First, it uses three central characteristics of the Thirty Years' War as a prism to describe and analyze current developments in the region. Second, it points to selected possible implications of such a development. In conclusion, it asks what these thoughts may mean for the prospects of a regional peace. By following these steps, the analysis looks beyond the IS and its immediate threat at the systemic shift that could be implied in its rise, a shift

that may best be described evoking the Thirty Years' War.

Omens of a New Thirty Years' War

The Thirty Years' War (1618–1648) was, in the words of Peter H. Wilson in his seminal work 'Europe's Tragedy', a 'struggle over the political and religious order of Central Europe'. This definition captures its importance for this analysis: The war was a protracted struggle, not a short, 'clean' war. It was a contest over the very concept of 'order', not just power within an order; it incorporated political as well as religious dynamics; and, finally, it engulfed the whole center of a continent, not just a distinct number of belligerent parties, let alone 'states'.

The war has shaped Europe's historical memory not only because of its length and immense cost, but because it was perceived even by contemporaries to have become a veritable self-feeding, self-preserving actor of its own, creating its own logic and evading Carl von Clausewitz' later (and, as is often forgotten, essentially normative) dictum that war had to be the extension of politics by other means; the Thirty Years' War ostensibly turned this logic upside down. Thus, it has developed into an *archetypal conflict* that stands in direct, and logical, contrast to the 'post-Westphalian' state-on-state wars that began to dominate in Europe

after the Peace of Westphalia in 1648 – and that still guide Western thinking on international politics.

In the following part, three elements of the 'Thirty Years' War' paradigm will be referenced to analyze current developments in the Middle East: The disintegration of order, the interaction of sectarian zeal and secular power struggles, and the emergence of a self-sustaining war economy.
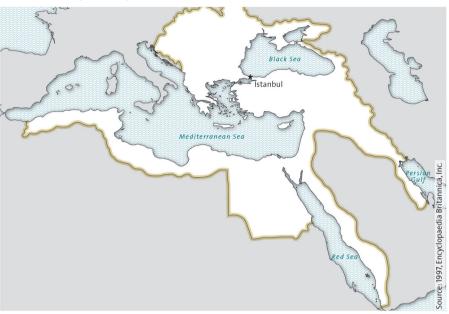
From Sykes-Picot to 'Syraq'

The Thirty Years' War saw a disintegration of Europe's geographic and political center. The Holy Roman Empire, always an entity only imperfectly described by today's political vocabulary, practically plunged into a civil war that saw an extensive redrawing of borders and open conquest for the sake of titles, rights, and territory. The war involved all of Europe, yet it was fought mostly – and most viciously – on the 'German' territory of the empire. This collapse of central power created a vacuum that was filled, at least partially, by stable, unitary, and determined outside powers, foremost among them France, Spain, and Sweden that protected their interests by sending their own armies or financing and supporting allied sovereigns and forces. A similar constellation – a disintegrating center that simultaneously constitutes the
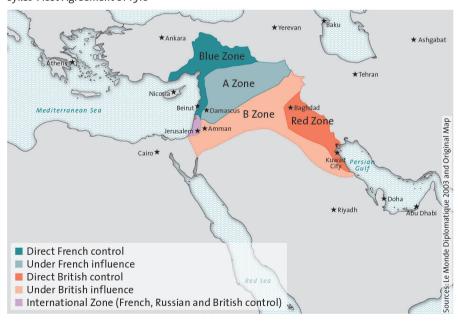
Evolution of borders in the Middle East

The Ottoman Empire at its peak

Source: 1997, Encyclopaedia Britannica, Inc.
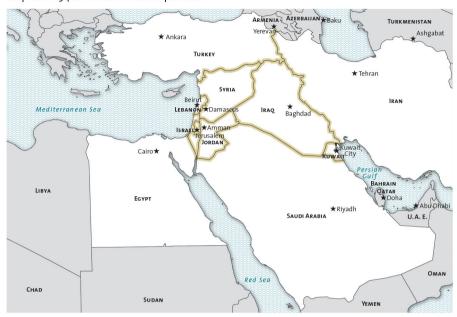
Sykes-Picot Agreement of 1916

Sources: Le Monde Diplomatique 2003 and Original Map

Legend:
- ■ Direct French control
- ■ Under French influence
- ■ Direct British control
- ■ Under British influence
- ■ International Zone (French, Russian and British control)
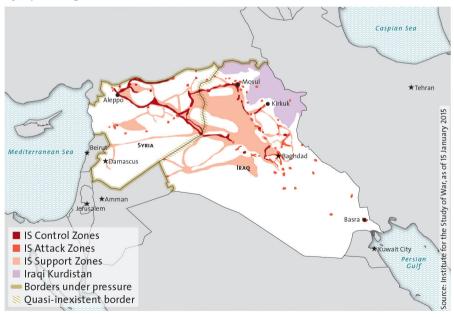
Map as of 1948: Territorial status quo ante

'Syraq': Disintegration of state borders

Source: Institute for the Study of War, as of 15 January 2015

main area of operations and the prize of the war, influenced significantly by outside powers with distinct political and sectarian agendas – may be looming in today's Middle East.

The modern Middle East – understood here as the region between Egypt in the west, Iran in the east and Turkey in the north – is still largely the result of the collapse of the Ottoman Empire following World War I and the resulting order predefined by the Sykes-Picot accord of 1916. In it, the colonial powers France and the UK reneged on earlier promises and decided to separate the region into spheres of influence. As a result, more often than not, they set borders and boundaries arbitrarily. Indeed, the very concept of Arab states in a modern sense developed in large part only after 1916 and against a colonial background. The geographical center of the Middle East – encompassing the Levant, Jordan, Iraq, and Saudi Arabia – consists of states whose very existence, let alone the demarcation of their boundaries, is thus a relatively young phenomenon. To subsequent generations of Middle Eastern leaders the colonial and often artificial nature of these borders was obvious, and efforts to render these borders obsolete are as old as these states themselves.

During the 1950s and 1960s, Pan-Arabism was a powerful force, propa-gating the unity of the Arab people while incorporating nominally social-ist elements of ideology. However, Arab unity never passed the test of reality. Hence, as young as they are, the borders between the Arab states have been the cornerstone of the regional order for nearly a century. While they have certainly not prevented conflicts and wars, they nevertheless contained them and mostly chan-neled them into state-controlled limi-tations. Fixed and recognized borders are a necessary condition for existing peace agreements in the region, and will have to serve as the foundations for those treaties for which there is yet some hope. Challenging current borders in the geographical center of the Middle East therefore means chal-lenging an order that has proven to be no principal impediment to peace and a suitable basis for regional stability.

'Syraq'

When, in June 2014, fighters of the IS commandeered a civilian Cat-erpillar bulldozer and cut a breach into the earth berm that marked the Syrian-Iraqi border, they symbolically challenged not only the current line separating both countries, but the whole concept of regional order. The IS thus most prominently embodies one of the characteristics most often described by evoking the Thirty Years' War – that of a disintegrating center

being contested and dominated by outside powers.

While many observers were surprised when IS forces occupied the Iraqi city of Mosul by *coup de main* in mid-2014, Syria and Iraq have long been de-facto parts of closely linked conflicts – so close that it does make sense, from an analytical and policymaking point of view, to consider Iraq and Syria as theaters of the same war, albeit with considerable differences when it comes to possible policy solutions. For all practical purposes, at the time of writing, a considerable part of the border between Iraq and Syria has ceased to exist and others like the Lebanese borders may follow. An increasing flow of money, weapons, fighters, and refugees threatens to render the pillars of Sykes-Picot obsolete.
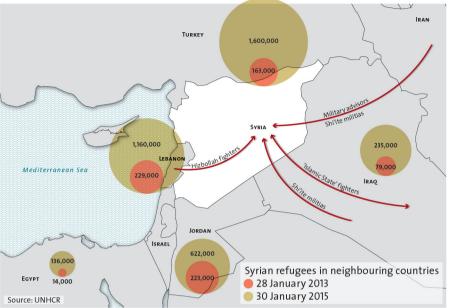
At some point during the Afghanistan war, it became policy for US officials in the administration of President Barack Obama to call the area of operations 'AfPak', thereby making clear that the conflict dynamics of Afghanistan and Pakistan are inextricably linked. At the risk of oversimplifying, for the analyst of both conflicts, it clearly makes sense to speak of the war in 'Syraq' to understand the interdependent genesis of the current situation while avoiding the pitfalls of meshing policy options for both countries.

Open borders: fighters and refugees
Even beyond 'Syraq', borders are set to lose their containing and structuring effect while states are in danger of losing every semblance of a 'monopoly of power'. The result is a massive two-way flow of fighters and refugees.

The war in 'Syraq' is fought primarily by non-state actors of varying character. As described above, the privatization of violence during the Thirty Years' War, partly in the form of mercenaries, was a major factor for both the duration as well as the fateful cyclical dynamic of violence that marked the war. It was far easier to raise armies than to disband them. First, disbanding mercenary groups necessitated funds that were often not available, which made it easier to keep those armies and satisfy them through resources generated by continued fighting. Second, years of continuous service produced a large number of men that never learned anything else but the craft of war, making a 're-integration' into society difficult at best. Third, the possibility of actively influencing the war solely by transferring money to professional mercenary leaders lowered the threshold of intervention and multiplied the number of parties and interests involved in the conflict. Similar dynamics can be seen in the current war. In fact, the majority of the heterogeneous Syrian

Flow of fighters and refugees from/into selected countries

war factions – the US had counted up to 1500 rebel groups by February 2014 – are dependent on international support in terms of money, personnel, and materiel. The conflict is thus by principle internationalized.

Furthermore, neither in Iraq nor in Syria does an undisputedly 'national' army exist. In Syria, the national army is widely perceived as an instrument of the Assad regime. The regime, for its part, depends heavily on aid from Russia and direct military support by Lebanese Hizbollah fighters, Iranian military advisors, and further Shi'ite militias composed, in part, of foreign

fighters predominantly hailing from Iraq, but also, allegedly, countries like Iran, Pakistan, Afghanistan, and Yemen. Various sources put the number of Hizbollah fighters at between 3000 and 5000, plus up to 5000 non-Syrian Shi'ite fighters. In addition, between several hundred and a few thousand Iranian military advisors are reported to be present on the ground.

The Syrian opposition, meanwhile, lacks an effective command and control structure. Thus, even the largest rebel 'groups', according to the International Crisis Group, resemble ad-hoc alliances of autonomous

groups more than effective military commands; they are more concerned about coordination, the de-conflicting of operations, and a relatively coherent external representation than they are about creating unity of effort, let alone unity of command. The primary rebel groups are the Free Syrian Army (FSA), originally made up of defectors from Assad's army, which incorporates secular or moderate Islamist groups and whose name suggests an organizational structure that does not exist in reality; more radical Islamist groups such as 'Islamic Front' and the Jaish al-Mujahideen; and, finally, openly jihadist groups such as Jabhat al-Nusra and the IS.

The dependence on external support is similar in Iraq. The Iraqi Army (IA) is heavily dependent on foreign assistance, especially from the US, which is supporting the build-up of new Iraqi divisions in 2015 to regain territory currently held by the IS. The integrative potential of the IA, meanwhile, is one of the main reasons for hope on the Iraqi side, where many Iraqis seem to prefer the army to sectarian militias, be they Sunni or Shi'ite. However, to have any chance on the battlefield, the IA still relies on support from these Shi'ite militias, many of which are allegedly supported by Iran or have strong ties to several figures within the cabinet of Iraqi Prime Minister Haider

al-Abadi. The Kurdish Peshmerga of northern Iraq, for their part, only lived up to their military reputation after receiving heavy support from US aircraft and are recipients of training and materiel provided by an international 'coalition of the willing', including Dutch, German, and British soldiers. Finally, the presence of Iranian military advisors on the ground on unspecified duties, and the ground attacks flown by Iranian aircraft, make clear that Tehran sees vital interests at stake and will have a role in any outcome of the fighting.

As of the beginning of 2015, the trend for external actors involved in financing non-state actors to protect their own interests continues. The US, after having delivered humanitarian assistance, training, and 'non-lethal' aid to some Syrian groups since at least 2013, is planning to equip and train up to 5000 'moderate' Syrian fighters to oppose the IS (and, possibly, the Syrian regime). In January 2015, reports suggested that Jordan, even before the killing of its pilot who had been captured by the IS, would start to finance militias in both Syria and Iraq to keep the IS from its borders and create a de-facto buffer zone.

Even more impressive than the numbers of fighters involved are the actual strategic and operational troop

movements throughout what is effectively a unified theater of operations. Reports describe movements of entire Shi'ite militia units from Iraq, where they became 'unemployed' after the US withdrawal in 2011, to Syria, lured by the promise of a solid salary, among other incentives. As those militias move from Iraq to Syria, Hizbollah units have been doing likewise since 2013, crossing regularly from Lebanon to Syria. The IS, for its part, moved units from Iraq into Syria after 2011 to gain combat experience and back again in force in 2014 for its summer offensive.

Finally, some reports indicate that in 2014, the IS ordered all members of its Libyan units to return to their home country to assist in the seizure of the port city of Derna in November of that year – in what would be a strategic movement of troops over hundreds of kilometers and through countries officially untouched by the war.

The flow of fighters through the region, a veritable back-and-forth of state and non-state forces, however, is eclipsed by the flow of refugees displaced by the war. Every neighbor of Syria is heavily affected by the war, if only through the arrival of Syrians fleeing the conflict. According to the United Nations High Commissioner for Refugees (UNHCR), by January 2015, 3,73 million Syrians had fled their country – out of a pre-war population of 22 million. Most refugees flee to Turkey (ca. 1,6 million), Lebanon (1,16 million), Jordan (622,000), Iraq (235,000), and Egypt (136,000). These numbers do not include those that travel further to European destinations, and they are expected to increase by another million to a total of nearly 4,3 million refugees in the course of 2015. In Iraq, the UNHCR in January 2015 estimated that 1,5 million residents were Internally Displaced Persons (IDPs) after more than twelve years of more or less continuous conflict.

The refugees are pushing a number of host countries to the breaking point, especially those that have always suffered from ethnical or religious tensions: Lebanon, a country that is continuously on the precipice of civil war and where the number of Syrian refugees has now reached the equivalent of a quarter of the country's pre-war population, felt compelled to introduce visa requirements for further refugees since January 2015, for the first time in decades, in a desperate move to re-establish the containing effect of its borders with Syria. Jordan, which borders both Syria and Iraq and furthermore is one of the pillars of the current order, notes with concern that the refugees now make up a full tenth

of its pre-war population. The Hashemite kingdom has a vivid memory of internal unrest in 1970 and is aware of the precariousness of a monarchy resting on the shoulders of what is effectively a national minority. Judging by the fate of the hundreds of thousands of descendants of the Palestinian refugees from the 1948 and 1967 wars, who have mostly never been able to establish themselves as full citizens in their host countries, the Syrian refugees might be a destabilizing factor for the regional order for decades to come.

Taken together, refugees and foreign fighters are part of the same phenomenon, namely the import and export of the conflict in 'Syraq' into the neighboring countries and its spillover beyond the original battleground. As states try to influence the war's outcome by supporting factions and militias, and at the same time struggle to maintain their physical separation from the conflict by strengthening their borders despite the inflow of refugees, these dynamics seem increasingly unsustainable.

Sectarian zeal and *raison d'état*
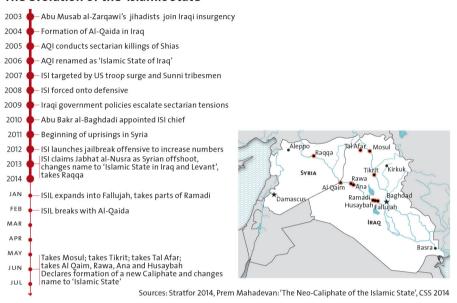
The Thirty Years' War was a religious war – or rather, it cannot be understood without taking into account the impact of religious reformation, in itself an immensely political process.

Major powers involved in the war, like Catholic France or Protestant Sweden, saw themselves more often than not as driven by religious imperatives, or even as vanguards in divine plans. Even where religious motives were not decisive, they were always at play. At the same time, however, the war saw one of the earliest and clearest manifestation of decidedly non-religious policies oriented towards a *raison d'état*: Most prominently, Catholic France under Cardinal de Richelieu, or Protestant sovereigns opting for alliances with the self-proclaimed vanguard of counter-reformation in Vienna. The war could not have started without religious fault lines, and it could not have lasted as long as it did without manifestly conflicting interests of states and sovereigns in a volatile environment, leading to alliances that were thought unlikely under pre-war constellations. It was this dualism of religious fervor and coolly calculating 'state' policies that contributed to the carnage of the war.

The same struggle between sectarian zeal and calculated state interest is obvious with regard to the countries that are at the same time most openly sectarian and most intimately involved in the war of 'Syraq'. Iran and Saudi Arabia have been the main regional contenders for hegemony in the Middle East for decades. While

The evolution of the 'Islamic State'

Year	Event
2003	Abu Musab al-Zarqawi's jihadists join Iraqi insurgency
2004	Formation of Al-Qaida in Iraq
2005	AQI conducts sectarian killings of Shias
2006	AQI renamed as 'Islamic State of Iraq'
2007	ISI targeted by US troop surge and Sunni tribesmen
2008	ISI forced onto defensive
2009	Iraqi government policies escalate sectarian tensions
2010	Abu Bakr al-Baghdadi appointed ISI chief
2011	Beginning of uprisings in Syria
2012	ISI launches jailbreak offensive to increase numbers
2013	ISI claims Jabhat al-Nusra as Syrian offshoot, changes name to 'Islamic State in Iraq and Levant', takes Raqqa
2014	
JAN	ISIL expands into Fallujah, takes parts of Ramadi
FEB	ISIL breaks with Al-Qaida
MAR	
APR	
MAY	Takes Mosul; takes Tikrit; takes Tal Afar;
JUN	takes Al Qaim, Rawa, Ana and Husaybah Declares formation of a new Caliphate and changes
JUL	name to 'Islamic State'

Sources: Stratfor 2014, Prem Mahadevan: 'The Neo-Caliphate of the Islamic State', CSS 2014

Tehran has, since 1979, often been an active exporter of Shi'ite revolution and activism, the currents underlying its involvement in the region reach much deeper to traditional dreams of Persian hegemony in its strategic neighborhood. This has both negative and positive implications: negative, in that the combination of geopolitical aspirations and religious zeal focusing on Shi'ite populations outside Iran is destabilizing and fuels the conflicts in the region; and positive, in that Iran is thus far acting within the framework of the current order, resisting changes to borders and focusing instead of influencing or dominating politics within those borders. It is here that a convergence of interests with other powers may be possible, as will be explained below.

Saudi Arabia, for its part, has continued its tradition of directing radical Islamist energies towards the outside lest it be endangered from within. It is determined to block Iranian moves towards hegemony and to prop up Sunni regimes and groups throughout the region. At the same time, Riyadh finds itself in the precarious situation of being in the midst of an immensely delicate succession after the death of King Abdullah in January 2015, coupled with an increasing threat of IS forces operating at its borders.

Even though Riyadh seems to be on the strategic defensive following Iran's push throughout the region, it might at some point decide that its interests are best served with a settlement on the basis of the territorial status quo – at least in the short term.

Two other neighbors of 'Syraq' will play a minor, yet still important role in any future development of the crisis. Neither is free from sectarian agendas, yet state interests appear to prevail, as of now. Turkey, under President Recep Tayyip Erdoğan, is heavily involved in the conflict both through the Syrian refugees it shelters and through the country's intense and deeply ambivalent relations with numerous opposition groups, the IS and the Kurds, in both Iraq and Syria. Ankara's call for a comprehensive approach to fighting the IS and its desire to stabilize Syria without Assad are born out of empathy with the largely Sunni resistance in Syria as well as the wish to see the refugees return – and therefore entirely pragmatic, a fact often overlooked by Western critics of Erdoğan.

Egypt, on the other hand, plagued by internal strife since the ouster of Hosni Mubarak and facing its own increasingly violent insurgency on the Sinai peninsula, has been the only major Arab power content with remaining largely aloof from the Syrian conflict.

This might even enable it to act as a mediator in any settlement – provided that groups and states allied with the Muslim Brotherhood do not profit. Taken together, both Turkey and Egypt would, in all probability, be prepared to sponsor a settlement based on a balancing of regional interests.

Looking beyond these four central states, both Jordan and Lebanon suffer from similar problems, though with varying intensity. Both are heavily affected by the war; yet, as minor powers, they are in no position to influence the war decisively, focusing instead on containing the possibly disastrous effects of an open spillover to their territory. Lebanon is on the verge of a renewed civil war, with Hizbollah and Sunni factions that are fighting each other in Syria barely keeping a fragile calm within Lebanon's borders based on the tacit agreement of all major Lebanese parties that a further spillover has to be avoided at all costs, making the state in the Levant a tense backwater of the war where fighters from both sides rest to recuperate. Jordan, meanwhile, is focused on securing its long border with 'Syraq', wary of its own population: though it may not be susceptible to the lures of the IS, its determination to fight for the monarchy against both internal and external enemies is far from clear. Considering

the reported support for armed tribes in 'Syraq' close to its borders and the cruel execution of the captured Jordanian pilot by the IS in February 2015, it seems doubtful, however, whether Amman can resist being drawn deeper into the conflict.

Taken together, all neighbors of 'Syraq' see vital interests affected, and all would have to bear the fallout of a disintegration of the current order. They are competitors, and may even be enemies, within the framework of the current order, yet they share the same interest of preserving this order and preventing the conflict that looms after a breakdown of the current balance. The question of whether secular, coldly calculated *raison d'état* can prevail over sectarian loyalties in those states will determine whether a comprehensive settlement on the basis of the status quo ante is possible at all.

Boom of a 'terror economy'

The years between 1618 and 1648 did not see continuous conflict, but rather a series of wars and campaigns. However, the war was perceived, already by contemporaries, as a period of continuous and existential instability. In the pre-state age of the mercenary, the war saw an extensive privatization of violence, with what could today be called non-state actors doing much of the fighting. Entrepreneurs of war, in-

cluding prominent commanders like Albrecht von Wallenstein, raised and led armies while making a huge profit from it. As a consequence, peace became less desirable for an increasingly powerful group of actors, while many 'ordinary people' lived their entire lives within a war economy that made service in some armed group the only realistic option for earning a decent wage – or at least to offer hope for spoils of war.

Today's Middle East sees the establishment of a veritable and hugely profitable war economy in 'Syraq'. Prem Mahadevan, in his chapter of this volume, details extensively the nexus between crime, terrorism, and non-state groups fighting in the region. Therefore, the following thoughts will be limited to a short assessment. With the advent of the IS exerting at least some part of control over large swathes of the region, this crime-terror nexus has been raised to a new level. What constituted smuggling, under the current order, may well qualify as trade in the years ahead. While the IS might be transitory, the economic quantum step it represents in terms of generating constant income under the conditions of, and through, structural instability, are likely to linger on after its demise. Moreover, the war economy transcends the war parties; as discussed, both individuals and whole militia units from both

sects are lured with respectable sums to 'enlist' in one group or continue their service in other parts of 'Syraq's' battlefield and beyond.

In addition, the presence of millions of refugees in the region is a fertile ground for an informal economy, as refugees are forced to work illegally if they can find employment at all. This will, in turn, further undermine the capacity of the states to generate income to support those very refugees. Once a full-blown trans-national war economy is in place, it will be immensely more difficult to revert to normalcy, as similar 'war societies' in Africa demonstrate convincingly.

Implications for 2015 and beyond

Status-quo vs. revisionist powers

The advent of the IS changes the potential dynamics of the conflict. The very concept of the 'Caliphate' announced by the IS in June 2014 poses a double challenge for the region today: First, it encompasses far more than Syria, in fact, it theoretically lays claim to the entire countries at one point in history ruled by Muslims. Second, the concept of the Caliphate, in its professed nature as a Muslim empire under God, stands in contrast to the philosophical concept of the Western state, at least within today's Middle East. The IS, through its (still distant, fragile, and barely functional)

Caliphate, is today's revisionist power par excellence.

For the regional powers, the advent of the IS and the threat of disintegration is existential: The wars of the last decade were waged over the control of states and regional hegemony, but within the paradigm of the current state-based Middle East. By establishing itself as a player in the conflict, the IS draws new lines between itself and the status-quo powers – including practically every state and regime in the region and beyond. Among those powers are, notably, even non-state actors like Hizbollah, quite remarkably for the resistance movement it claims to be.

It is no coincidence that this emerging constellation is in the interest of the Syrian regime. The mid-term goal of the Assad regime seems clear: To consolidate the area under its control at the cost of the mainstream opposition, after which it would be militarily strengthened and could present itself as the only realistic alternative to a jihadist opposition and thereby as a potential partner for the West and regional powers. Assad's regime is thus positioning itself as the one force that could defend the status quo (ante), the current regional order and its borders, against the revisionist force of the IS. In doing so, it is

banking on the common interest of all current powers – and Assad may well have calculated correctly. In short, the advent of the IS has not brought peace any nearer, but it may have raised the likelihood that an eventual peace will be based on the smallest common denominator of most parties – the reestablishment of the state-based order.

Fragile Iranian hegemony

Iran has, so far, been the great winner in the turmoil that has beset the region since 2003, as the last years have seen the advance of Iranian proxies throughout the Middle East. In Lebanon, no political issue can be decided against objections of Hizbollah; in Iraq, Tehran has secured a government dominated by Shi'ites, and it has the last word on most matters of importance; and in Yemen, Shi'ite rebels allegedly supported by Tehran appear to have the upper hand in a violent struggle for power in Sana'a. However, as impressive as Iran's influence in the region is at the beginning in 2015, it stands on shaky ground, and it is not at all clear that this influence can be transformed into the regional hegemony that Tehran aspires to. Two factors are reason enough for skepticism.

First, in economic terms, Iran is relatively weak, suffering from years of increasingly effective international sanctions and, lately, the punishing effects

of the drop in world oil prices. Iran is estimated by the IMF to need an oil price of USD 131 to finance a balanced budget; at the time of writing, the price hovered around USD 50. As Anthony Cordesman has noted pointedly in a study for the Geneva Center for Security Policy (GCSP), Iran's economic performance is already dwarfed just by the combined GCC states – not taking into account the other Sunni Arab states not at all friendly with Iran.

Second, and more important, in a region made up of overwhelmingly Sunni Arab states and people, Shi'ite Iran is an outlier. It cannot hope to dominate the region against a united front of Arab states; therefore, its only hope lies in dominating the states individually through Shi'ite proxies, either in the form of regimes or through de-facto independent forces like Hizbollah. This proxy-based hegemony is inherently unstable, fuels a violent sectarianism, and would in no way resemble the long-term structural hegemony that many observers fear. It is here that the IS constitutes a paradoxical threat to Iran: The instability caused by the war benefits Iranian involvement through proxies; however, a collapse of the state-based order would be detrimental to Iranian interests, as it needs those states to dominate the system.

Against this background, as Iran is engaged in nuclear negotiations with the international community, it is once again clear why a negotiated nuclear threshold status would be immensely beneficial for Iran. It would ease the economic burden while likely preventing the regional nuclear arms race Tehran fears. While it wishes to continue its delicate course of fueling instability within states without challenging the existence of those states, Iran has a vital interest in its own domestic economic stability. A New Thirty Years' War, therefore, would have very ambivalent implications for Iran, offering historic opportunities while simultaneously threatening the very basis of its rise.

Prospect of new alliances

The disintegration of traditional order and the fragmentation of the political and social landscape may, over time, lead to a shift in alliances that would seem paradoxical as of today.

One factor is the above described dynamic of pitting status-quo powers against revisionist movements. That will concern state as well as non-state actors. While Israel has been a rather passive observer of the war, so far, and is therefore not dealt with extensively here, it seems possible that Tel Aviv may one day see strong incentives to support Hizbollah – the quasi-state devil it knows – against jihadist groups

at its borders. The events of January 2015, with Israel reportedly supporting Jabhat al-Nusra on the Golan Heights, only confirms the basic dynamic: That of a state practicing 'realpolitik' and leaving all options on the table. In the event of a viable nuclear accord between the P5+1 and Iran, a strategic rapprochement between Tel Aviv and Tehran may well be a viable, if most likely informal policy option for both states.

A further element is the ambiguous status of outside powers. In the face of strategic uncertainty over the future involvement of the US and continuous speculation over an increasing role of China in the region, it would be naive to assume that current parameters of intra-regional relations will stay consistent over the next years and decades. Cracks between Israel and the US might not be as transitory as is often asserted if the structural rightwing majority in Israel solidifies further; Turkey has proven to be an either unreliable or volatile partner for nearly every state; and Saudi Arabia may increasingly make its strategic calculations without the US alliance as a *conditio sine qua non*. The center of the Middle East is disintegrating, peripheral powers are oscillating, and external powers are facing fundamental strategic decisions – new alliances therefore seem more than likely.

Conclusion: A Westphalian Peace?

After 30 years of bloodshed and immense destruction, the Peace of Westphalia ended the war in 1648 in what could be termed a 'great compromise'. The peace was at its core a positive affirmation of the old order. It cemented shifts in power, but no revolutionary outcomes. Plus, in a striking acknowledgement of its international dimension, both France and Sweden were formal parties to the new constitution, and thereby de-facto guarantors of it. Finally, the peace settled the religious feud on the basis of a simple insight that lay at the basis of every compromise since the Peace of Augsburg in 1555: That, at least for the time being, no sect could possibly prevail.

That is telling for today's Middle East. First, no peace in Syria is possible without the consent of its neighbors. A final settlement may reflect realities on the ground and gradual changes in the relative power of the region's states; however, it will not be possible against the persistent objection of any one power, first and foremost Iran. This conclusion, which may seem sobering at first, points to possible pathways out of the conflict, provided that all parties get a seat at the table and all interests are perceived as inherently legitimate. The main UN-sponsored peace process of Geneva and Montreux that

failed in January 2014 did not fulfill these criteria. Second, the basis of such an understanding could be an informal understanding of the 'status-quo powers' – in essence, all involved states plus Hizbollah – that any prolongation of the conflict could simultaneously destabilize themselves and strengthen revisionist powers such as the IS. Thus, a common interest of the region's powers could be the preservation of the state-based order. That, of course, necessitates that all powers come to this very basic insight; and that, at least for the time being, state reasoning should trump sectarian agendas, if only for pragmatic reasons.

These conclusions might seem theoretical in nature, and unhelpful in practice. That may be true; but as long as those minimal requirements are not met, it appears that the violence in 'Syraq' will continue; that the parties to the conflict (minus the IS) will fight to position themselves for negotiations to come; and that temporary and partial cease-fires are liable only to strengthen the party with strategic or operational superiority if the other side cannot replenish itself. Until a comprehensive settlement is reached, localized initiatives seem destined to fail – as they did between 1618 and 1648. ●

Putin's Russia: exploiting the weaknesses of liberal Europe

Jonas Grätz

Russia's aggression against Ukraine has brought war back into Europe. In addition, it presents a threefold challenge to an already weakened liberal Europe: With regard to security, Moscow has spoiled the EU's approach of transforming its neighborhood while disregarding the power of military coercion. Furthermore, Russia's President Vladimir Putin can also exploit the existing weaknesses of the EU's economic policies and the waning enthusiasm for the EU's liberalism in member states. Collectively, those challenges result in a crisis of the EU's liberal order.

Russian President Vladimir Putin, Defense Minister Sergei Shoigu (L) and Russia's Federal Security Service (FSB) Director Alexander Bortnikov (R) watch events to mark Victory Day in Sevastopol, 9 May 2014.

In the run-up to 2014, Europe was preparing to commemorate the start of the First World War. The overwhelming mood was one of a chastened look back on a very different past that Europe has long left behind. One year later, Russia has annexed Crimea, robbing a piece of land from a post-Soviet country. Even more strikingly, it keeps fuelling a war that has killed thousands on the battlefields of Donbas. As events in Ukraine mirror broader disagreements between Russia and the West over the perception and the future of the European interstate order, fears of further military escalation have been revived.

The conflict eludes any consensus of the two sides. The EU emphasizes that Russia's actions have undermined the core principles of the European security order such as the 1975 Helsinki Final Act and the 1990 Paris Charter that had stabilized peace since 1975 and had settled the Cold War. Moscow believes that these rules have become outdated as they do not reflect Russia's position as a great power but instead helped to spread Western institutions, such as the EU and NATO. Thus, where the EU argues that sovereign states are free to join alliances, Russia sees a threat to its own survival as a great power, engineered by the EU and the US. Hence, Russia's main aim is to devise new rules and principles

that would prevent Western structures from coming even closer to the homeland. To achieve this, Putin is eager to weaken Western institutions and to benefit from any emerging split between Western European nations as well as between them and their transatlantic partners.

The central argument of this chapter is that the EU's liberal order is in crisis, as existing weaknesses are being exploited by Putin's Russia. Moscow is confronting an EU that is militarily unprepared; it aims at exploiting the EU's growing economic divergences, and it is deliberately targeting an already fraying domestic political consensus. This constitutes a threefold challenge in the spheres of security, economy, and political ideology.

Liberalism, with its focus on individual autonomy and rights as constituting principles of order, has been the blueprint of the EU's integration model. It has allowed the EU to become a forward-looking project that aims to overcome historic and geographic determinism. By crafting common rules, the European world would become less discrete and more 'flat' and accessible to individual activity. Europe would not have a common past, but a common future. This vision is challenged by Putin's traditionalist revisionism, by the failure to

overcome economic crisis, and by the resulting return of the nation inside the EU.

With regard to security both sides have strikingly different perspectives on international relations, and there is no agreement over principles. Thus, while the security situation in Europe may not be militarily as threatening, it is nonetheless more volatile than during much of the Cold War. The EU has so far failed to improve its military capabilities, remaining a soft power in a more and more 'hard-power' world. It is thus liable to continue in the shadow of NATO for the years ahead. This, however, enables Putin to target the transatlantic link and stir underlying anti-American sentiments.

Economically, liberal economic integration has failed to bring about the necessary political convergence, as highlighted by the persistent Euro crisis. Economic imbalances have been strengthened between and within countries, giving rise to envy, resentment, and disenchantment with integration. As Germany has emerged as an economic powerhouse, effectively bankrolling other European countries, the old problem of German power in Europe has resurfaced. European integration and the Euro were conceived to hold the specter of German domination at bay. Germany's

strong position is therefore grist to the mill of those who think of the EU in terms of power politics rather than in institutions. This both encourages and justifies strategies of bandwagoning with Moscow, undermining the EU's unity.

Politically, a chauvinist and illiberal alternative to mainstream and pro-EU parties has arisen on the back of economic problems. Playing on resentment against a 'German Europe' and the US, they oppose the EU's most important institutions, such as the Euro and the free movement of people and services, instead seeking salvation in a Europe of sovereign, self-sufficient nations. Needless to say, these parties stance enjoys Putin's monetary and ideational support. Similarly, they see Russia as a partner for a future European order, based on nation-states. This limits the EU's space of maneuver towards Russia and poses questions over the durability of the EU and its commitment to liberal order.

This chapter will focus on how Russia has exacerbated both of the EU's crises, external and internal, and how the EU has reacted to these challenges. It will therefore first outline why Putin's Russia, as a 'postmodern absolutist state', presents an existential threat to the EU. Second, it will look into the

crisis of Europe's external security, of its economic principles, and of its political ideologies, which in turn prove to be open doors to be exploited by a determined Russia. Third, in conclusion, it will take a look at what this might mean for the years ahead.

A systemic challenge: Russia's postmodern absolutism

As indicated in last year's Strategic Trends, the Russia that annexed Crimea poses a distinct systemic challenge to the EU. To understand Russia's actions, it is not appropriate to focus on theories of great-power competition. Russia's behavior is governed by the country's domestic order and associated constraints rather than the laws of international relations.

Russia's order today can best be understood as a form of postmodern absolutism. It combines absolutism's traditional elements – a single ruler with a strong coercive capacity, a belligerent army, a subservient economic class, mercantilist economic policy, and a subservient church – with the postmodern notion that reality can be constructed in the mass media. With the help of communication technology, the absolute ruler can construct his or her own reality in order to maintain power. Hence, postmodern absolutism relies less on coercion of the masses than on their manipulation. Also,

Orthodox faith is only one source of legitimacy; while Russia is being positioned as a traditionalist, anti-Western great power in order to legitimate the regime.
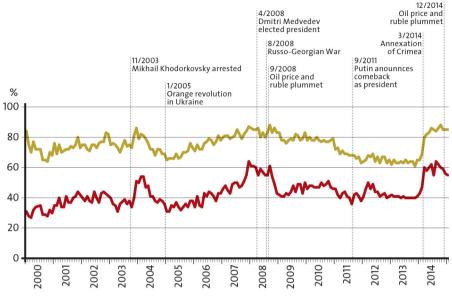
Postmodern absolutism works for Putin, as Russians despise the authorities, yet overwhelmingly believe that their country is a great power that has to be supported at any rate. Hence, Putin can muster support from the population as long as he can present himself as defender of a Russia that is great, but under threat. A great Russia must never show weakness. Putin's weakness would become evident if he tried to reform the economy. His re-ideologization is thus defensive and experimental; he is acting out of anxiety rather than out of strength.

Popularity is Putin's main focus, and it hinges on showing strength. This also implies that his actions will depend on the resistance he encounters. To remain in power, Putin therefore has two main tasks. For one, he has to nurture the basic foundations of Russia's identity as a traditional great power. It would be shattered if Ukraine or other neighbors with close ethnic and historical ties adopted a Western trajectory. Second, Putin must constantly prove that Russia is a great power. Hence, he increased funding for the military. Also, he

Political support in Russia

Approval of Putin and the general situation in Russia

11/2003
Mikhail Khodorkovsky arrested

1/2005
Orange revolution
in Ukraine

4/2008
Dmitri Medvedev
elected president

8/2008
Russo-Georgian War

9/2008
Oil price and
ruble plummet

9/2011
Putin anounnces
comeback
as president

12/2014
Oil price and
ruble plummet

3/2014
Annexation
of Crimea

— Do you approve of Putin's activities as the President (Prime Minister) of Russia?
— Is Russia moving in the right direction or is this course a dead-end?

Source: Levada Center
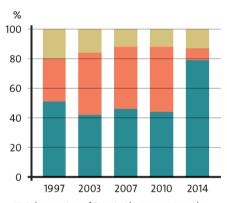
founded the Eurasian Economic Union in his effort to talk with the EU on equal terms. In Ukraine, both of these tasks converge: It is the most vital neighbor for Russia's great power identity and is engaged with the rival EU. If Ukraine adopted a different path, the underlying narrative and the potential to shore up power vis-à-vis the EU would be in tatters. It is these tasks of ensuring regime security that dominate Putin's policies, rather than abstract notions of 'national security interests'.

But Putin's dependence on popularity also means that there are limits to his actions. Two factors have made Putin hesitate in Ukraine. First, the appetite for conducting war is checked by the risk of casualties. So far, these have been limited as Putin has been able to arm volunteers from Donbas, Russia, and elsewhere. However, a broader war would necessitate greater involvement, which would have an impact on Putin's rating. Wanting to believe in propaganda is one thing, especially if it is favorable to one's own cause,

but should he decide to sacrifice the lives of thousands of Russian sons and husbands, a different propaganda effort would be necessary. Another weakness is the economy: Economic decline will over time reduce the resources that Putin can bring to bear – both internally and, crucially, also to prove Russia's capabilities as a great power. Therefore, were the conflict only about Ukraine, the challenge to the EU would not be existential; however, as is argued below, it goes well beyond the Donbas.

Anti-Western sentiment in Russia

What do you think, the biggest Western countries (USA, Germany, Japan, UK and others) – are those partners or opponents of Russia?

%
100

80

60

40

20

0

1997 2003 2007 2010 2014

■ Adversaries of Russia that want to solve their problems on its account and infringe on Russia's interests at every convenient opportunity.
■ Partners of Russia that have common interests (in the fight against terrorism and crime, environmental protection, in the development of science, culture, and the economy.
■ Difficult to answer.

Source: Levada Center

The roots of the conflict in Ukraine run deep – at the fundamental level, it is also a systemic conflict between the antagonistic political orders of a liberal EU and Russia's postmodern absolutism. The orders produce different fears: EU leaders fear nothing more than military conflict, and Putin fears nothing more than the breakdown of his regime. On the contrary, Putin's Russia has proven to have a higher tolerance for war, obviously accepting physical coercion as a substantive element of power. This is why he has the upper hand over the EU as long as he can extract concessions by waging a limited war.

Security: the military's power to frustrate

Putin's embrace of postmodern absolutism has led to conflict with the EU. Not limited to Ukraine, this struggle presents the first real challenge in decades to the security of EU members as well as to its 'soft security' focused external policies. Worse still, the conflict in Ukraine came unexpected: The EU was lulled by its transformative success in Eastern Europe and on the Balkans, assuming an apparent liberal consensus where there was none. Meanwhile, Europe seems to have lost the ability for strategic, politico-military thinking that prevailed during the Cold War. The EU has now been forced to acknowledge

that it needs a credible 'stick' to complement the economic 'carrots' of its liberal agenda.

A hard landing for the 'soft' neighborhood policy

Traditionally, the EU's policy towards its eastern neighborhood has been stimulated by the more or less successful waves of enlargement. But while it was strong on its ambition to transform new members and extend the liberal order to further regions, its key flaws have always been a lack of resources and incentives. This ambiguity reflected policy disagreements in the EU: Whereas some members, such as Poland and Sweden, were strongly in favor of a robust policy or even offering membership to Ukraine, continental Western Europe had largely succumbed to 'enlargement fatigue', whereas Southern Europe was essentially indifferent.

It was only after Russia's war against Georgia in 2008 that the EU decided to shift up a gear. The argument was that the countries left in between Russia and the EU should be given more attention in order to reduce Russian leverage. Hence, the EU negotiated ambitious association agreements that would help those countries to transform into liberal market economies. However, the EU still wanted to offer those countries an alternative to

Russia on the cheap: enlargement fatigue prevailed – the agreements did not provide for the free movement and settlement of people. Fear of work migration and competitive pressure were among the main reasons why the EU still did not hold out any membership perspective.

Matters of hard security went totally unheeded, leading to a grave miscalculation. Some even thought that the EU offer would be the catch-all solution to regional problems: Purportedly, it would not be seen as a threat by Russia, unlike NATO, while it would assuage the states to the east. Nevertheless, hard security soon came to trump the EU's offers: Those partner countries dependent on Russian security guarantees, such as Armenia, had to cease cooperation.

When Putin turned to Ukraine and annexed Crimea, the EU was supportive of Kyiv, but still loath to confront Russia directly. Economic interests are strong for many members, as is Russia's outsized diplomatic role in many of the world's arenas. Even more important was the general desire for friendly relations with Moscow in many corners of the EU. This is joined by considerations of power politics in some small EU countries that see Moscow as a partner to balance against an EU dominated by large states.

It is notable that even the Visegrad states of Central Eastern Europe were not coherent: Warsaw was hawkish, whereas Prague, Bratislava, and Budapest joined Western Europe in prioritizing the economy. Initial sanctions were symbolic as a result, mostly targeting political relations and individuals. More 'hawkish' EU members, mostly Poland, Sweden, and the Baltics, were placated with a three-stage plan to eventually escalate sanctions.

It took the Kremlin's excalation in the Donbas to galvanize the EU. The decisive catalyst came on 17 July 2014, when what were probably Russian forces accidentally shot down Malaysian Airlines Flight 17 with a BUK anti-aircraft missile. Now, Germany came around in support for sanctions and took the lead in coordination. This was supported by the UK, the Netherlands, and eventually France. The smaller dissenting states could no longer resist the general trend. At last, the EU was ready to impose financial restrictions against selected banks and companies, as well as export restrictions for military, dual-use, and certain energy extraction technologies.

The EU's growing firmness, joined by a tanking oil price, did not go unnoticed with Putin. Firstly, while his goals remain unchanged, he went back to the negotiation table to agree on the Minsk protocol in September 2014. As this did not end the fighting, Putin limited himself to a comparatively light footprint in Donbas and concentrated on destabilizing Ukraine rather than on a full-fledged assault. Secondly, the worsening economic outlook in Russia has reduced Putin's resources at home and abroad, even though the population has so far rallied behind the leader. Disillusionment among the middle class and the elite may grow over time, making Putin more amenable to negotiations with the West over kick-starting his economy.

However, in February 2015, Putin again sensed an opportunity. Some of the sanctions were soon to expire, and the EU's internal political crisis was bleeding into foreign policy: Elections in Greece had added a firm voice of resistance to renewing, let alone thinking of further sanctions. Thus, a new ground offensive by the separatists was again supported with the latest Russian equipment. Putin's basic logic continues to produce results: Every day the war continues, Ukraine grows weaker as a state and the EU loses out on establishing a workable regional order.

Hard security: Washington, the savior?
Under any scenario – continuing with a liberal neighborhood policy or accepting Russia as a great power in
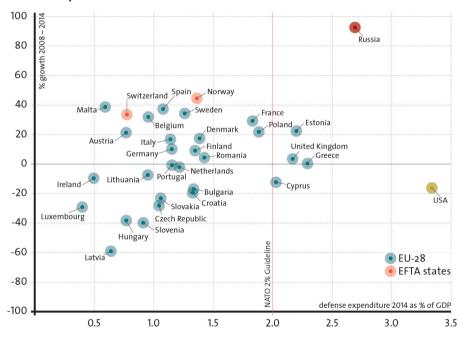
Europe – the EU's member states would need strong military forces. However, the EU's military power is weakening in the wake of economic crisis. To be sure, the conflict has brought hard lessons with regard to the continued utility of military force, but these have not, as of now, translated into a higher commitment to military affairs. Even after the events in Ukraine, most EU members are still reluctant to increase their below-norm defense budgets.

This has only added to the EU's traditional 'Venus' character: Attempts at

making the EU a full-fledged security actor have fallen flat. The European Security Strategy dates from 2003. Military cooperation between EU members has been affected as well: Franco-British cooperation, the most ambitious partnership, is lingering due to budgetary constraints and conflicting political agendas. Only small members such as Sweden and Finland are trying to build up closer military ties. As a result, after years of trying to build a common European defense capability, NATO and thus the US are still the main guarantors of European

Defense expenditures of selected countries

Sources: IISS Military Balance 2009 and 2015

security. This trend has only been reinforced by the Ukraine crisis – not so much because the US wanted to, but rather because many EU leaders do not have many viable alternatives. Facing the choice between a well-known US role as security provider and Russia's preference, a 'multipolar world order' with its inherent instability, many naturally opted for the former.

However, doubts remain whether the underlying premise of the renewed pivot to the US is credible, which might reinforce instability. The priority that the US attaches to European defense is uncertain, given the Pentagon's already stretched commitments, turmoil in the Middle East, and Washington's increasing strategic introspection. Nerves are frayed in Eastern Europe, and Putin may be tempted to test the US commitment to those countries. In any case, the outsized role ascribed to the US in the defense of a majority of EU members allows Russia to conveniently equate the EU with NATO and the US, which provides fuel to a regional conflict and pushes it right up to the global level, elevating the stakes. It also adds fuel to Russia's propaganda machine in the EU, where many are made to believe that the EU is being dragged into a conflict that is in Washington's interest.

On balance, the EU's security is in a dangerous limbo. If the EU wants to uphold its liberal order, it either needs unambiguous assurances from the US about its future long-term commitment, or it must start investing into a higher military profile itself. If things continue as before, the low profile of NATO's European members and the uncertain US outlook might well invite Russia to test the commitment of major EU member states and of the US to defending Eastern Europe and the Baltics.
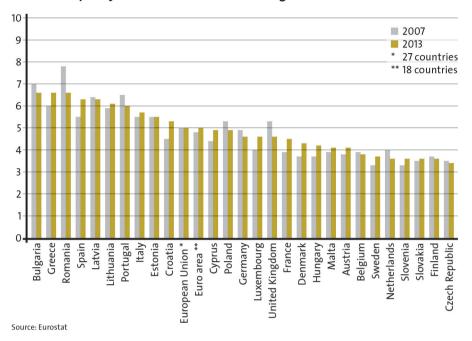
Economy: dividing the EU

While Putin's Russia faces the EU from outside, its economy is a challenge coming from within. Having started as an economic project, the EU might also fall due to economics – most vividly expressed in the continuing crisis of the Euro, which is weighed down by heavy public debt burdens. The lagging growth is only a syndrome, however. More severe for the political coherence of the EU are the growing divergences between EU member states. Those, in turn, are driven by the underlying political blockades that have been further deepened by the crisis response policies. These policies and their economic effects have undermined the EU's legitimacy in the eyes of large parts of the European population. The lack of economic performance also supplies additional arguments to those that look towards Moscow as an alternative to Brussels.

Income inequality before and after the sovereign debt crisis

Source: Eurostat

The EU's crisis response: fuelling realism
When the Euro crisis hit in 2008, not many countries were keen to take a lead: France had a high debt load and rising unemployment rate itself. Italy was hit hard by the crisis. The role of crisis manager thus fell to Germany. Germany was ready to provide the EU's financial assistance with the necessary firepower, but together with its northern partners, it demanded strict reforms and spending cuts in return. Five years on, unemployment and poverty have declined to a long-term low in Germany, while the opposite has happened in Southern EU countries, especially in Greece. This has undermined the trust in the EU.

Worse still, the crisis response policies, while technically and morally justified, were in part self-defeating. They had a counterproductive effect on the ability of the periphery to reform: Contributing to higher inequality, they undermined societal readiness to accept reform. Instead, they fuelled fears of social decline and mistrust of elites. As argued below, this has given rise to radical right- and left-wing alternatives.

The EU's concrete policies contributing to these trends were the bank bailouts, austerity, and quantitative easing. First, bank bailouts were designed in a way that emphasized the responsibility of states and discounted the responsibility of creditors. Hence, taxpayers in the EU and especially the crisis states were held responsible, while the financial system and its decision-makers were saved. Only in the case of Greece did private creditors have to accept a 'voluntary haircut' – equal to only one-eighth of total Greek debt. While there might have been good systemic reasons to bail out the banks, this policy was the 'original sin' of crisis response with long-term distributional consequences. This precedent can also be used to agitate against the EU as representing the interests of financial markets.

Second, the austerity policies that have been negotiated by the Troika of the EU, the International Monetary Fund (IMF), and the European Central Bank (ECB) foresee a radical reduction of expenses and structural reforms to put the state budget on a positive long-term trajectory. Usually quite heavy on the expenditure side, these programs again tend to impact mainly the middle classes and the poor rather than the rich, amplifying the effects of the economic crisis. This is all the truer as the rich successfully exercised their power to avoid accountability in crisis-ridden states – which is an issue wholly unrelated to the Troika policies. For example, it is estimated that wealthy Greeks hold the equivalent of 65 per cent of their country's GDP in assets abroad.

Third, the ECB's quantitative easing is a concession to periphery states. It was not officially supported by Germany and is intended to somewhat reduce the impression of German domination of the EU. The ECB's main trick is to buy government bonds so that their yield stays low, regardless of the risk perceived by market actors. The economic results are excess liquidity and ultra-low or negative interest rates. The latter penalize savers and future pensioners – again, the middle class. Excess liquidity has to be invested somewhere, which elevates asset prices. Hence, stock and property owners profit. The only positive effect for the poor may be in terms of investment and employment rising due to a weakened currency, but investment has not been boosted so far.

The EU thus finds itself in a vicious circle. Countries have to improve competitiveness, but the EU's policy responses to the crisis have further worsened the societal foundations needed to achieve it. To be sure, local elites are also to blame. But the policies followed by the EU under German leadership have constituted

a useful target for those who prefer to view the EU as an imperial project, weakening its coherence.

Putin's economic attraction

With the EU in a profound economic and institutional bind, and helped by the growing divergences, Putin's Russia holds considerable attraction as a partner for trading and balancing against German influence. This has already weakened the resolve of the EU when it comes to sanctions. It also bolsters those who want to sacrifice the existing European order for the sake of profits.

To be sure, the crisis in Ukraine and the falling oil price have somewhat weakened Russia's economic soft power for the time being. The South Stream gas pipeline, Russia's main project in the EU, is an obvious casualty of the conflict. With this pipeline, Russia planned to divide and rule by attracting the Balkans and Central European countries economically. But the financial sanctions and the worsening outlook for Russia's Gazprom have killed the project.

Nevertheless, Putin has not given up on his game of 'divide and rule': Now, he is trying to capitalize on the new government in Athens, choosing Greece as the new end point of the proposed gas pipeline to Turkey. The tactic is always the same: Promising construction

contracts and transit revenues, Russia lures its partners to toe a pro-Russian line in the EU, be it with regard to foreign policy or energy laws.

While the EU's sanctions and Russia's counter-sanctions did not have a large impact on overall growth, they do impact local economies. The reduction of economic cooperation with Russia is an easy target for those forces critical of the EU. The sanctions thus add to the prevalent criticism of the EU's economic policies. The rise of alternative elites and their non-mainstream parties is now driving this point home – with a little help from Putin.

Politics and Putin: ideological subversion

The economic crisis with its growing imbalance between EU countries has led to a political backlash against the EU and the liberal ideology it stands for. As liberalism puts the individual with its freedom and rights in the center, it breaks down traditional communities and identities that act as stabilizers. This tends to be compensated if liberal markets are perceived to bring overall benefits, as individuals adopt a positive, progressive outlook on the future. If markets do not deliver enough benefits, however, the balance tilts against liberalism: Fear of decline and distrust of elites results in renewed calls for community.

As the EU has never been able to foster a 'thick' identity with redistributive institutions, this call is directed at the nation-state. As a result, demands are heard for 'real' national elites that will reinstate borders and protect the nation instead of following the demands of global markets. The EU is being hit twice: Both as a liberal project that has been advocating the completion of the internal market since the Maastricht treaty, and as a supranational institution, because demands for national sovereignty do not mix well with the spirit needed to make common institutions work. This feebleness of the EU's ideology is again being exploited by Putin's Russia.

The rise of anti-mainstream parties

The EU's party landscape is witnessing a rapid transformation. Anti-mainstream parties from the right and left are rising, and they are forming new lateral partnerships on an illiberal and social axis. In Northern Europe, far-right nationalism is on the rise, which is often directly opposed to EU membership. In Southern Europe, where austerity is the defining feature of life, nationalist left-wing parties are more prominent. All of them promise a return of politics, 'real change' instead of the endless administration of political life under current governments. As the Syriza-ANEL coalition government in Greece illustrates, there is not much enmity between left and right. While they disagree on identity politics and chauvinism, both agree on their state-centric and social agenda, as well as their staunch opposition to the US and the EU.
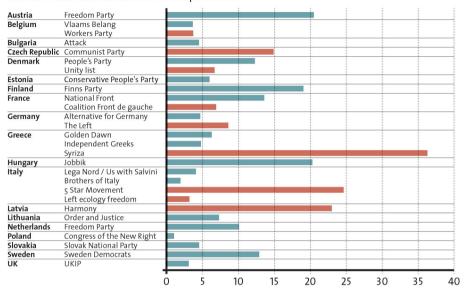
Far-right nationalist parties react to the fears of solitary economic decline. Taking their cue from Putin, they seek to revitalize the community of the nation with its traditions as a source of inspiration and mobilization. Muslim immigrants are often the main target, while the EU is a secondary target limiting national autonomy. Far-right nationalists are now the third-largest force in France, the Netherlands, Austria, Greece, Denmark, Finland, and Sweden. In the UK, France, and Denmark, they won the 2014 elections to the European Parliament, EP, while the 'Alternative for Germany' came fifth. Those parties either want to leave the Schengen Agreement, the Euro zone, and the EU, or substantially renegotiate existing treaties so as to minimize the impact of transnational cooperation to the bare minimum level, for example, to fight crime. To make the renovated national home more comfortable, most of them vow to invest strongly in social protection of the elderly.

In Southern Europe, which is suffering from austerity and a profound malfunctioning of its state institutions

Selected anti-mainstream parties in the EU

Results in last national elections to the parliament

Country	Party
Austria	Freedom Party
Belgium	Vlaams Belang
	Workers Party
Bulgaria	Attack
Czech Republic	Communist Party
Denmark	People's Party
	Unity list
Estonia	Conservative People's Party
Finland	Finns Party
France	National Front
	Coalition Front de gauche
Germany	Alternative for Germany
	The Left
Greece	Golden Dawn
	Independent Greeks
	Syriza
Hungary	Jobbik
Italy	Lega Nord / Us with Salvini
	Brothers of Italy
	5 Star Movement
	Left ecology freedom
Latvia	Harmony
Lithuania	Order and Justice
Netherlands	Freedom Party
Poland	Congress of the New Right
Slovakia	Slovak National Party
Sweden	Sweden Democrats
UK	UKIP

(x-axis: 0 5 10 15 20 25 30 35 40)
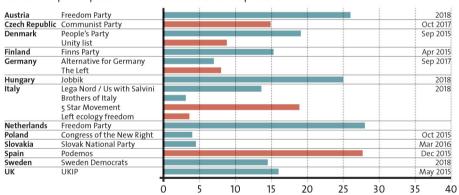
Results in opinion polls on national elections to the parliament

Country	Party	Date
Austria	Freedom Party	2018
Czech Republic	Communist Party	Oct 2017
Denmark	People's Party	Sep 2015
	Unity list	
Finland	Finns Party	Apr 2015
Germany	Alternative for Germany	Sep 2017
	The Left	
Hungary	Jobbik	2018
Italy	Lega Nord / Us with Salvini	2018
	Brothers of Italy	
	5 Star Movement	
	Left ecology freedom	
Netherlands	Freedom Party	
Poland	Congress of the New Right	Oct 2015
Slovakia	Slovak National Party	Mar 2016
Spain	Podemos	Dec 2015
Sweden	Sweden Democrats	2018
UK	UKIP	May 2015

(x-axis: 0 5 10 15 20 25 30 35 40)

■ Right-wing
■ Left-wing
Dates on the right hand indicate scheduled next election

Sources: National election bodies; for opinion polls: Austria: Der Standard / Market, Feb. 2015; Czech Republic SANEP s.r.o., June 2014; Denmark: Voxmeter, February 2015; Estonia: Turu-uuringute AS, March 2015; Finland: Tietoykkönen, February 2015; Germany: Infratest Dimap, February 2015; Hungary: Ipsos, February 2015; Italy: Termometro Politico, 11.2.2015; Netherlands: Ipsos, February 2015; Poland: CBOS, 11.2.2015; Slovakia: Median SK, August 2014; Spain Metroscopia, February 2015; Sweden: Svensk Opinion Nu, February 2015; UK: Lord Ashcroft Polls, February 2015.

and elites, more 'progressive' causes are taking root. Some parties, like comedian Beppe Grillo's 'Five Star Movement' in Italy, which came in second in both national and EP elections, rally against the mistrusted institutions of representative democracy, but do not have an elaborate ideology that would let them take up the key questions. Grillo's success is not likely to last.

More traditional left-wing parties rallying for a strong welfare state and against the 'austerity diktat' are likely to have a more profound impact. The landslide victory of Alexis Tsipras's Syriza in the 2015 Greek elections will have repercussions in Spain and Italy. The concessions that he will be able to extract will also be demanded elsewhere. In Spain, the leftist Podemos movement draws heavily on Tsipras's experience and is now the most popular party, having come fourth in the EP elections.

Interestingly, strong anti-systemic parties are not easy to be found in the new EU member states of Central Eastern Europe. For one, the economic crisis has hit them less severely or has been overcome quicker due to the better societal cohesion. Secondly, Muslim immigration is not an issue in these societies. Third, the mainstream parties have traditionally been more inclusive of Eurosceptic attitudes

and social conservative values. Hungary, where radical ethno-nationalist and anti-Semitic Jobbik party is the third-largest political force, is an exception.

Putin: investing in a new Europe

For Putin, these new anti-mainstream parties represent a huge opening in his effort to undermine the EU. They are exactly the force that he needs for realizing his goals: They are mostly opposed to the US and NATO, while advocating stronger ties with Russia. In most cases, they also want to dismantle the EU, striving for a Europe of self-sufficient sovereign nation states instead of rules-based integration. Ideologically, they are on the same line, emphasizing at least resistance to global capital and at most adherence to the same traditional values. This would allow Russia to re-emerge as a great power with its own sphere of influence, and to wield greater influence in Europe. Even if such parties do not come to power, they will lead to a more cautious approach in the EU too, as they will be a credible threat to existing elites.

The love is reciprocal – most of the alternative elites to the right and left of the spectrum exhibit sympathies for Putin's Russia. For one, they see him as a truly sovereign ruler who has resisted the anti-political forces of an

US-dominated global market. Ideationally, they are fond of him for cherishing national traditions over liberalism and multiculturalism. Thus, for many alternative elites, Putin is coming to the rescue as the white knight in their 'anti-imperialist' fight against the US-based Western order and its 'lackeys' in Brussels.

Putin's support for anti-mainstream parties comes in three ways: informational, organizational, and financial. Informationally, the parties profit from Putin's propaganda networks such as the TV station RT. They grant extended coverage to the party leaders and their views, as well as portraying key common enemies, such as the US and global capital, in a negative way. Organizationally, the Russian ruling party United Russia has developed strong ties to many of the anti-mainstream parties and sends members to their party congresses. The party leaders are also regular participants in Russia-based political conferences, discussing possible layouts of an alternative Europe. Financially, the EUR 9 million loan of the Russian-owned First Czech-Russian Bank to the French Front National stands out.

The Ukraine crisis and the unity that European leaders have shown over the war in Ukraine have further alienated the inherently anti-Western parts of the electorate, giving the same parties an additional boost. With the victorious 'lateral coalition' of left- and right-wing parties in Greece, the days of EU unity over Russia may now be counted. Putin's investment in political alternatives may soon pay off.

In general, the emergence of anti-mainstream parties has already caused a political shift to the right, as a strategy of marginalization and defamation can only serve as a temporary fix. The preferred strategy of leaders has been to adopt part of those parties' agenda, as can be seen in the UK or in Hungary. While this stance undermines the EU's principles such as freedom of movement, the swing to the right has largely been grist to the mill of the alternatives.

Conclusion: EU leaders at a crossroads

The current crisis of liberal Europe is grave, rocking the EU to its very foundations from without and from within. Externally, it is about the ability of the EU to establish a workable order in the neighborhood. So far, EU leaders have failed to come to grips with Putin's ambition to create a different Europe based on relations between the great powers. Internally, the EU's liberal approach to order is questioned as well

– both by the economic divergences between member states, and by the political movements arising on their back. This rise of anti-establishment parties and governments shows that functionalist integration has run its course and politics can no longer be ignored. The war in Ukraine connects all of those three challenges, as it resonates deeply inside the EU and acts as a booster to the prevalent internal problems. Acting on those challenges, Putin has intentionally deepened the EU's crisis.

The crisis now compels the EU's leaders to prioritize, to concentrate on the essence, and to make decisions. To some extent, this has already happened over the war in Ukraine: The severe, even though belated sanctions on Russia are a positive sign of unity. But that unity remains very fragile, and more resourceful efforts would be needed to solve the huge task of establishing regional order. Internally, the rise of anti-mainstream parties has become acute in Greece. While this poses many challenges, the new government has also one main advantage: The greater trust of voters, which would allow them to implement the reforms that the EU needs.

The downside risks for the EU are huge. If the alliance of far-right and left-wing 'anti-imperialists' were to gain additional ground, the Eurozone might unravel. The EU itself would become more and more blocked by disputes, with smaller regional integration projects arising on the continent. In any case, Russia would emerge as one of the new centers, realizing its dream of a Europe based on great powers. The new era could be marked by instability on a greater scale and on more dimensions.

Conversely, if the EU pulls together and embraces a forward-looking discourse that reaffirms its basic values and backs them up with resources, it may emerge stronger from the crisis. This would prevent Putin's Russia from emerging as a key actor on the European scene and transforming the regional order. It would also transform the challenge itself: Russian politics has always mirrored developments in Europe, and the decline of the EU has empowered those advocating a traditionalist and isolationist Russia. An EU that re-emerges stronger and more united from this crisis is thus the best precaution against a belligerent Russia.

Resurgent radicalism

Prem Mahadevan

The growing profile of the 'Islamic State', and its rivalry with al-Qaida, has heightened fears of terror attacks on Europe. The group has injected new enthusiasm into the global jihadist project by declaring itself a 'Caliphate' and thereby creating an illusion of military progress relative to the operationally stagnant al-Qaida. Europe needs to brace itself for the dual task of combating threats to its citizens at home while remaining alert to the strategic implications of Islamist insurgencies overseas.

Belgian soldiers patrol outside the European Commission headquarters in central Brussels, 17 January 2015.

A spate of terrorist attacks in the West since summer 2014 has alerted analysts to a fresh wave of radicalism from the Middle East. The rise of the so-called 'Islamic State' (IS) in Iraq and Syria is the most visible explanation of this phenomenon, but its roots lie deeper. 'Leaderless jihad', wherein terrorist groups devolve long-range operations to unaffiliated amateurs, has developed a forward momentum alongside 'territorial jihad', which aims to seize control of government structures. The two types of insurrectionary doctrine are complementing each other at a global level, confronting the West with a simultaneous threat of lone-wolf attacks at home and Islamist insurgencies in the developing world.

Although the IS is by far the most important contributor to this trend, its impact needs to gauged holistically. The group has profited from a growing sense of disillusionment among the international jihadist community with its main rival, al-Qaida. The latter was conceived and designed to operate from the sanctuary of a benevolent state or states, which it enjoyed when some governments were prepared to shelter its operatives for geopolitical reasons during the 1990s. Since the attacks in the US on 11 September 2001, however, the group has been homeless in a political sense. This has adversely affected its capacity to

strike the West directly or to project influence into the Middle East. While many jihadist ideologues continue to stand by it, a younger generation of radicals has emerged since the 1980s that finds al-Qaida an antiquated brand. These younger radicals are gravitating towards the IS.

The January 2015 attacks in Paris are illustrative of the amorphous nature of contemporary jihadism. While the gunmen who attacked the satirical newsmagazine *Charlie Hebdo* claimed affiliation with al-Qaida in the Arabian Peninsula (AQAP), their accomplice who seized hostages in a kosher supermarket declared loyalty to the IS. From later reports, it seems as though all three men were operating semi-autonomously as products of a jihadist sub-culture that pushed them towards acts of violence, *sans* any concrete political grievance. Based on this event – as well as others in Europe, Canada, and the US – security officials have begun to wonder whether jihadist networks in the West are actually more of a mutated youth gang problem, instead of a coordinated terrorist offensive, requiring a bottom-up policing and community engagement solution.

What cannot be disputed, however, is that within its own neighborhood, the IS is coordinating military operations

with the aim of creating a micro-state. The group's capture of Mosul in June 2014 was a tremendous source of inspiration for jihadists across the world who had yet to score a comparable victory over government forces in their own regions. Since then, the IS' foremost emulator seems to be Boko Haram in Nigeria, which has become even more ruthless over the last year. As was the case in Iraq, an increased willingness to inflict civilian casualties has terrorized large parts of the Nigerian state security apparatus, allowing jihadists to substantially undermine governmental authority. A corollary to this has been a significant growth in the role of organized crime in supporting jihadism – having acquired political dominance in certain pockets of territory, groups that were previously engaged in smuggling can now claim to be engaged in 'trade', and what was previously extortion can slowly be redefined as 'taxation'.

There are thus, four explanatory pillars that account for the resurgence of radical Islamism. The first is the IS, and the alterative that it presents to the borderless model of jihad hitherto waged by al-Qaida. The second is al-Qaida itself, along with its affiliated groups. The third is the phenomenon that is loosely known as 'lone wolves' – individuals sympathetic to the cause of jihadism, but operating alone and with no formal training. This phenomenon has also produced 'amateur' jihadists – individuals who have received some training from an established group, but who operate autonomously and whose statement of subordination to that group is purely formal. The fourth pillar is organized criminal activity, which provides vital financial support for terrorist attacks.

This chapter will analyze how the rise of the IS has impacted, and will continue to impact, international terrorism. It will first situate the IS within global terrorism trends, to illustrate how these are being shaped by the group. Then, it shall demonstrate that the IS is feeding into an underlying pattern of governance collapse that exists in other parts of the developing world. This collapse has allowed the group to co-opt specialist talent into its ranks, giving it a structured and bureaucratic quality that makes its eradication all the more difficult. Next, the chapter will outline how the IS has diversified its funding sources to become a financially viable shadow state, taking particular advantage of its territorial dominance to generate revenue from new sources that are normally accessible only to governments. Finally, the chapter will examine the threat that developments in the Middle East and North Africa directly pose to European security.

Global overview

More than 13 years since the beginning of the 'Global War on Terrorism', the US and its allies have yet to fully destroy a single jihadist group. While al-Qaida Central – the core network originally formed in 1988 by Osama bin Laden and currently led by his deputy Ayman al-Zawahiri from Pakistan – has been severely damaged, it remains a functioning entity. Other groups have either voluntarily scaled back operations against the West, such as Hizbollah since 2001, or maintained a focus on regional targets instead of hitting Western homelands. For the most part, the US has been content to accord lesser priority to combating these groups, being preoccupied with homeland security and the vagaries of domestic politics.
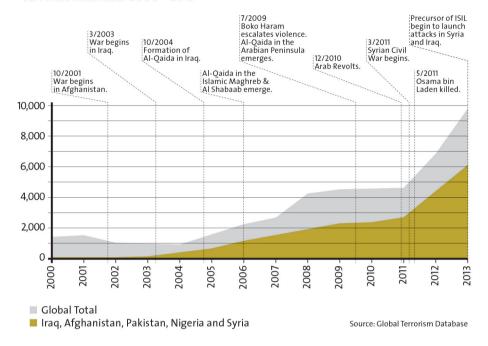
The IS has emerged in this gap between the global rhetoric and local reality of US counterterrorism – the group harms Western overseas interests, far from Western jurisdictions, where the political will and operational means to combat it are proportionately weaker. Its media statements indicate that it perceives the US as averse to waging long-drawn counterinsurgency campaigns, and believes that it can outlast US air and even ground attacks. Despite heavy losses, the notion of persistence is central to its narrative. Here, it has history in its favor.

Even as US troops were withdrawing from Iraq in 2011, the IS was struggling to cope with 95 per cent manpower losses, which had been incurred as a result of cooperation between the Iraqi government, the US military, and Sunni tribesmen who opposed its hardline ideology. Between 2007 and 2010, the group fought a losing battle in which its leaders were tracked and killed, and its operational commanders scattered into the desert. However, its reconstruction began even during its downfall, when a number of cadres came into contact with former Iraqi military officials being detained at US-run prison camps. The result was a potent fusion of Salafist ideology with professional knowledge of army counterintelligence and urban warfare tactics.

In contrast, after 2011, the US lacked on-ground human intelligence assets in Iraq to push back against the jihadist momentum. This became evident during the first weeks of Operation Inherent Resolve, the aerial bombing of IS positions that began in summer 2014. Most sorties failed to engage any target, due to lack of identifying data. Although subsequent strikes were quite effective, notably around Kobane in Syria as a result of target-spotting by Kurdish militia, overall, the limited impact of airpower has been demonstrated. As already mentioned in *Stra-*

Terrorist incidents 2000 – 2013

10/2001
War begins
in Afghanistan.

3/2003
War begins
in Iraq.

10/2004
Formation of
Al-Qaida in Iraq.

Al-Qaida in the
Islamic Maghreb &
Al Shabaab emerge.

7/2009
Boko Haram
escalates violence.
Al-Qaida in the
Arabian Peninsula
emerges.

12/2010
Arab Revolts.

3/2011
Syrian Civil
War begins.

5/2011
Osama bin
Laden killed.

Precursor of ISIL
begin to launch
attacks in Syria
and Iraq.

Global Total

Iraq, Afghanistan, Pakistan, Nigeria and Syria

Source: Global Terrorism Database

tegic Trends 2014, jihadists across the world have learned since 2001 to cope with the threat of aerial attack. Recognizing this, US officials have recently voiced concern that al-Qaida Central has proven surprisingly resilient against drone strikes in Pakistan. With the IS committed to carving out its own sovereignty in the Middle East, the question is now how al-Qaida can be prevented from adopting a similar agenda in South Asia once the US presence in Afghanistan ends completely.

No doubt some precautionary measures need to be taken against a further rise in terrorist violence. Worldwide, such violence has risen five-fold since 2000, with 95 per cent of all deaths occurring in non-OECD countries. This latter statistic indicates that Islamist insurgencies quantitatively represent a much bigger threat to international security than 'lone wolves' in the West. During 2012–2013, fatalities increased by 61 per cent; the corresponding rise in 2013–14 was roughly another 25 per cent. Most attacks have occurred in just five countries: Iraq, Syria, Afghanistan, Pakistan, and Nigeria. All are states where jihadist groups have a history of

fighting for territorial dominance, and in some cases, exploiting local politics to propel their own institution-building agendas. In Libya, it is estimated that as many as 1700 militias are battling for supremacy, providing the IS with multiple entry points into the country through loaning its Libyan cohorts to local Islamists. The capture of Benghazi by Ansar al-Sharia in August 2014 and the subsequent declaration of an 'Islamic Emirate' there is viewed as the result of just such a process.

Furthermore, jihadist violence is proliferating largely independently of al-Qaida Central. A study of 664 terrorist/insurgent operations in November 2014 found that over 60 per cent of all fatalities were caused by groups that had no formal connection with the core al-Qaida network based in Pakistan. Worldwide, local jihadists are estimated to carry out 20 attacks daily, killing almost 170 people. This happens whether or not their organizational leaders have sworn a loyalty oath to al-Qaida chief al-Zawahiri. Such oaths, in fact, might only be an instrument in the power struggle between al-Qaida and the IS that could ratchet up their competitive dynamic.

During the 1990s, Osama bin Laden built a network of al-Qaida affiliates through two means: providing training and obtaining loyalty oaths from

the leaders of more established groups. His successor al-Zawahiri inherited this network, but allowed parts of it to atrophy, particularly in Africa. Thus, the Nigerian group Boko Haram came to look for alternative patrons, eventually finding one in the IS. The two groups have created what appears to be a symbiotic partnership: in exchange for deferential statements from Boko Haram, the IS encourages African jihadists who cannot travel to Syria or Iraq, to go to Nigeria instead. Both organizations have enslaved women and girls, in particular from the Christian community in Nigeria and the Yazidis in Iraq. They justify such acts by claiming women as war plunder, to be bartered and sold as concubines. By specifying that they are targeting non-Muslims, they adopt an uncompromisingly exclusivist posture that appeals to other jihadist groups waging regional insurgencies. Attacks on Christian minorities in the Middle East and Africa increased substantially in 2014 over the previous year, more than doubling the world total.

Although al-Qaida is in no way averse to the brutal tactics of the IS, it disagrees with the group regarding their strategic value. Al-Qaida's leadership has tended to be sensitive to Muslim public opinion and therefore, at least at the rhetorical level, advocates

restraint in targeting co-religionists. The IS, on the other hand, is not only openly sectarian, but adheres to a rigid interpretation of Islam that allows it to openly brand all who disagree with it as apostates worthy of being killed. A very broad targeting policy gives the IS more opportunity to demonstrate its presence than al-Qaida, which is now regarded with disdain by a new generation of jihadist sympathizers, looking to align with a group that has a successful operational track record.

There is a fundamental difference between al-Qaida and the IS that partially explains their differing trajectories and fortunes. Al-Qaida saw its own role in global jihad as being merely a facilitator in the re-establishment of a grand Caliphate rather than being the founder. The IS, however, sees itself as the Caliphate's foundational core, which means that it is willing to take responsibility for governance – something al-Qaida never did, even when it enjoyed safe haven in Sudan and Afghanistan in the 1990s. Al-Qaida is a parasitic organization that needs to be protected by a state structure. With no state willing or able to shield it from US counterterrorism efforts since 2001, the relevance of its strategic concept to the international jihadist project has dwindled. The IS seemingly offers a solution: creating a micro-state in regions of poor

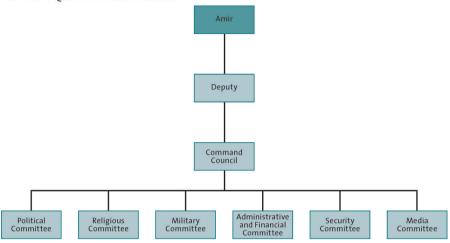government presence that can serve as a platform for imposing a rule of puritanical Islam.

Terrorism through governance

After setbacks in 2007 – 2010, the resurgence of the IS was enabled by the Syrian civil war and the simultaneous rise of sectarian politics in Iraq. Syria provided the group with a hinterland, in which to build an operational base. Thereafter, the IS initiated two campaigns: 'Breaking the Walls' and 'Soldiers' Harvest' intended to free its cadres who were being held in Iraqi prisons and to assassinate government officials, respectively. Even as it was thus engaged, the Shi'ite regime of then Prime Minister Nouri al-Maliki systematically alienated Sunni Arabs by excluding them from job opportunities and refusing them any method of peaceful protest.

What resulted was a Sunni tribal uprising; the IS quickly jumped on the bandwagon and turned it to its own advantage. By forging tactical alliances with Sunni militias, it built pockets of influence in the Sunni heartland away from the Syrian border through relatively sophisticated, intelligence-led operations. In the north, it gradually encircled and infiltrated Mosul, paralyzing the local administration while keeping the Baghdad government off balance through a relentless

Al-Qaida and 'Islamic State' hierarchy

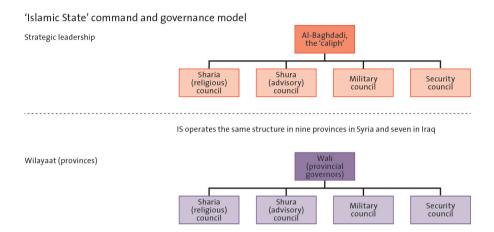Pre-9/11 Al-Qaida command structure

Source: Rohan Gunaratna & Aviv Oreg (2010), 'Al Qaeda's Organizational Structure and its Evolution', *Studies in Conflict & Terrorism*, 33:12, p.1055 (adapted by the author)

car-bombing campaign. When the group finally occupied Mosul in June 2014, its clandestine networks in the city had already done the job of scaring away local security forces commanders and exploiting sectarian rifts in the army. The actual occupation was thus achieved relatively easily.

Such meticulous organization and planning had originated from the former Iraqi army officials who joined the IS while imprisoned alongside its ideological leaders in 2007 – 2010. Their circumstances were peculiar to Iraq: left with no source of income after US occupation forces disbanded the Ba'athist political infrastructure, many fell in with insurgent groups.

The tactical acumen of these former soldiers when combined with the fanaticism of radical Islamist ideologues, made for a lethal combination as violence in Iraq steadily increased. Admittedly, such a convergence of interests is unlikely in other jihadist hotspots across the world, but even a limited overlap of agendas is enough to change the dynamics of a conflict. The top IS commander in Syria, for example, is thought to be an ethnic Chechen who previously served in Georgian military intelligence. Many of the battlefield successes attributed to jihadist groups in Syria are believed to have been orchestrated by veteran insurgents from the Caucasus. A decade of experience in fighting Russian

'Islamic State' command and governance model

Strategic leadership

Al-Baghdadi, the 'caliph'

Sharia (religious) council | Shura (advisory) council | Military council | Security council

IS operates the same structure in nine provinces in Syria and seven in Iraq

Wilayaat (provinces)

Wali (provincial governors)

Sharia (religious) council | Shura (advisory) council | Military council | Security council

Qitahaat sectors (local districts)   Same structure repeated at local level

Source: BBC IS investigation team

troops has made Chechen Islamists tactically adept, to a degree unusual among foreign fighters travelling to the Middle East. This has allowed them to assume a disproportionate number of senior positions within the anti-Assad forces in Syria.

Even without the help of former soldiers, jihadist groups are gaining potency through skill-sharing among themselves. In 2003, the IS (then known by a different name) pioneered suicide bombings in Iraq. It had learned the efficacy of this tactic from al-Qaida, which in turn had acquired it from Hizbollah in the early 1990s. At the start of its bombing campaign in Iraq, the IS was in a junior partnership

with al-Qaida. Over a period of time, the power balance shifted, as al-Qaida languished under the weight of international counterterrorism pressure, and the IS engaged in indiscriminate attacks against Iraqi Shi'ites, Sunnis, and US occupation forces. Its much more visible presence in the conflict area allowed the group to develop an independent funding stream from foreign donors, which then attracted recruits from the wider Middle East and beyond.

The recruits were a mix of jihadist veterans from other combat theaters and new volunteers. Initially motivated by a desire to drive out Western troops from Muslim lands, over a decade, the

53

influx morphed into a quasi-criminal assortment of freebooting mercenaries. Many had criminal convictions in their home countries. For example, a number of Lebanese-Australians who had been involved in street gang violence left to fight in Syria after 2011. Chechen exiles from Turkey and Austria, among other countries, found the IS as a natural home for their jihadist sympathies. Over 100 Kosovar Albanians – part of an ethnicity that has tended to be staunchly pro-Western out of gratitude for the NATO intervention of 1999 – joined the IS and Jabhat al-Nusra in Syria.

What unites the motley crowd of foreign fighters with the IS, al-Qaida, and regional jihadists is a common quest for a new political identity that cuts across current international and regional boundaries. The IS has moved to the first rank of jihadism by building a governance model that many Islamists find attractive after perceiving themselves as marginalized in their home societies. Disillusionment with a lack of integration into local power structures has made groups such as Boko Haram, Abu Sayyaf and Mujahidin Indonesia Timur, as well as factions of al-Qaida in the Islamic Maghreb, keen to adopt new tactics for seizing power. Boko Haram, for instance, has shifted from guerrilla attacks to clearing and holding territory

in the face of Nigerian government offensives. It has seeded approach routes to its strongholds (roughly 20 towns in three states) with improvised explosive devices (IEDs), much as the Taliban have done in Afghanistan, to drive up the human and material costs of counterinsurgency. Apparently copying the IS, it has targeted the Shi'ite community in Nigeria with the aim of polarizing intra-Muslim relations and creating a captive constituency among Sunnis. The group is also feeding into the historical identity of ethnic Kanuris who once ruled over an Empire founded in the modern-day province of Borno. Its transborder operations into Cameroon and Chad are a repudiation of current nation-state boundaries, just as the IS is meant to signify a rejection of the Sykes-Picot agreement.

The IS has used the retreat of governance in Iraq to set up its own administration, the first objective of which is counterintelligence. Accounts from IS-controlled territories suggest that the group prioritizes the identification of government loyalists and religious minorities when it enters a new area. Computerized databanks have been created, based on financial records and government files, to identify persons who might pose a security risk to the group. Besides coercing municipal workers to continue their

jobs (with pay), the IS also assigns some of its foreign volunteers to administrative duties, thereby showing that it is committed to bureaucratization. The group matches volunteers to their aptitude and previous career training, and has even put out job advertisements for oil industry experts. Allegedly, the IS eventually hopes to print its own gold-supported currency, thereby strengthening its claim to full statehood. Towards this, it is reported to have established its own bank in early 2015 and announced a 'budget' of USD 2 billion, the bulk of which has been allocated towards salary payments and civic service provision.

Al-Qaida cannot hope to match this. With the IS having appeared amidst the jihadist fraternity, it now faces a loyalty problem among its affiliate groups. Some jihadists that operate in conflict zones believe that the IS model is more applicable to them, particularly since they do not share al-Qaida's long-standing fixation with attacking Western homelands. Others, probably out of organizational inertia and lack of past contacts with the IS leadership, are inclined to abide by their vows of loyalty to al-Qaida chief al-Zawahiri. The IS itself is believed to be courting defections from the latter camp, creating factional tensions. One example is the Dagestan network of the so-called 'Caucasus Emirate' in southern Russia.

While the bulk of the 'Emirate' has remained loyal to al-Qaida, a powerful sub-group is thought to have switched allegiance to the IS. The implications of this are two-fold: Either the mainstream 'Caucasus Emirate' will now be compelled to emulate the IS model and attempt to set up a parallel administration, or it will seek to carry out expeditionary attacks on Russian cities to compensate for its overall military weakness. In any case, Russian authorities are prudent in anticipating a rise in terrorist violence.

Diversified funding through territorial dominance

A jihadist group with at least partial control over territory can substantially increase its fund-generating ability by taxing legal and illegal business activity and/or smuggling high-value contraband in bulk quantities. The IS has leveraged such control to become the richest terrorist group in the world, with a total worth of roughly USD 2 billion. Al-Qaida Central, on the other hand, has been systematically starved of funds since 2001. In 2005, it even had to ask the IS (then known as al-Qaida in Iraq) for USD 100,000. In the following years, the IS' strategic fortunes rose in tandem with its finances. From initially relying on private donors in Sunni Arab states, the group entered the lucrative oil-smuggling trade. It thereby acquired

an independent funding base that lay well outside the jurisdiction of US law enforcement agencies. This put it at an advantage over al-Qaida, which depended on long-distance money trails that were being aggressively targeted by financial counterterrorism measures.

The IS symbolizes a convergence between organized crime and terrorism. During the Cold War, both terrorists and gangsters received some measure of protection from state authorities in order to function. This protection often only amounted to passive tolerance and nothing more, but without it, they had no hope of survival. Thus, Palestinian terrorist groups like the Black September Organization were covertly sheltered by the intelligence services of Warsaw Pact countries, while the West allowed organizations like the Sicilian Mafia to establish parallel states in post-war Italy, intending to use them to thwart the spread of communism. After 1989, both arrangements collapsed. Terrorist and criminal organizations on both sides of the Cold War ideological contest found themselves simultaneously orphaned, and began collaborating with each other on a more frequent basis. As outsiders in the new international system, they had little to lose.

Scrutiny of terrorist funding over the last two decades reveals that mercenary imperatives can forge alliances across all ideological boundaries. For example, during the early 2000s, Hizbollah obtained weapons from Russian mobsters in Central America. Introductions were provided by a former Israeli military official who had grown friendly with a senior Hizbollah operative through business ties developed in the Congo. Shi'ite Hizbollah had also helped Sunni al-Qaida enter the West African diamond smuggling trade during the Liberian civil war. More recently, it is believed that al-Qaida in the Islamic Maghreb (AQIM) has grown heavily involved in the Latin American drug trade. In exchange for protecting cocaine shipments travelling across North Africa and bound for Europe, the Algerian jihadist group is reportedly paid a 15 per cent commission on the profits.

Other groups in Africa obtain funding from charcoal exports (al-Shabaab) and maritime piracy (Boko Haram). None of these is exclusively dependent on one source of income. Depending on local conditions, it can also be possible to abduct Western nationals who are either visiting as tourists or working in the country as technical experts or NGO activists. From 2008 to 2014, governments paid anywhere between USD 125 and 165 million in ransoms for hostages taken by al-Qaida affiliates around

the world, the majority of them in the Maghreb. Exact figures are difficult to obtain since many Western countries disguised the payments as 'foreign aid money'. The actual kidnappings were done by local criminals who were paid a commission for each snatch. Victims did not always have to be foreigners: In South Asia, the Pakistani Taliban has for several years run a kidnapping racket focused on businessmen, politicians, and government officials. Intelligence on prospective targets is obtained through domestic servants. Understaffed law enforcement agencies, worried for the safety of their own personnel, tend to take a hands-off approach, often advising victims' families to negotiate a ransom on their own.

The scale of rent collection by terrorist groups is directly related to their territoriality. Two of the biggest funding sources of the IS are peculiar to the Middle East: oil and antiques. Before the US-led aerial bombing campaign of its forces, the IS was estimated to be capable of producing 280,000 barrels of oil per day, of which it actually sold only 80,000. This alone is thought to have yielded a daily income of USD 1 million. Oil sold at half the market price to neighboring countries made the IS inherently competitive as an energy producer – hence, much of the coalition's effort has since gone into attacking its oil installations. These are likely to

have suffered serious damage by early 2015, causing a shift to other sources of revenue generation. Antiques play a crucial role here: the archaeologically rich terrain of Iraq and Syria literally offers a treasure trove of diggings. As with kidnapping and drug trafficking, the actual theft is often done by professional smuggling syndicates, with the IS content to accept a tax of at least 20 per cent of the profits. Satellite imagery of countries affected by the Arab Revolts of 2011 has indicated a massive rise in the number of illegal excavations of archaeological sites. While not all of these are related to jihadist violence, there is still a strong suspicion that the trade in artifacts, which ends mainly in European and US auction houses, is fuelling terrorist activity in the Middle East.

Drug and human trafficking and antique smuggling are favored by jihadist groups because they have a dual purpose: to generate operational funds and to harm the 'enemy' politically. Since the 1980s, Islamist terrorists have justified involvement in the global drug trade as a way of undermining Western societies, which they perceive as morally degenerate. With the IS now in physical control of territory in the Middle East, sex slave trading has become a tool for asserting political dominance in local cultures. Even antique smuggling is seen

as part of a 'cleansing' process, to rid the IS of pagan idols that contravene its core religious principles and legitimacy. To their supporters, there is little contradiction in jihadists being pious but waging war against non-believers through street-level crime. In the absence of state sponsorship as the major source of funding it had been during the Cold War, social acceptance of profiteering in the terrorism industry has increased.

The result has been an increase in the operational capability of terrorist groups, which can now develop ties with organized crime for sustained logistical support. Although the actual costs of conducting a terrorist attack in the West are relatively low, contact with criminal elements is essential for any sophisticated and large-scale operation. Even if such contact is delegated to secondary members of the jihadist network, it remains vital because its absence would drive up the logistical expenses of an attack to levels that might not be within reach of the core operatives. For example, the 2004 Madrid bombings are estimated to have cost approximately EUR 8000, but the indirect costs of clandestine travel and supporting activities would have been at least five times that figure. Some of these hidden costs were collaterally absorbed by criminal syndicates such as the Italian Camorra, allowing the

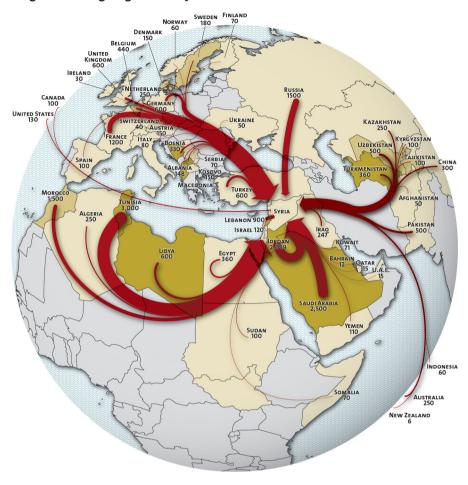attack cell to concentrate on the actual bombings.

In recent years, Europol has been particularly alarmed by high levels of illegal immigration from conflict-prone countries in the Middle East and South Asia. Among diaspora communities, illegal elements of the Pakistani diaspora might be the most susceptible to fusing crime and terrorism. This is partly because of the strong role that Pakistan plays in the Afghan heroin trade, serving as a transit country for 40 per cent of all shipments. Rivalry between different trafficking syndicates, often based on nationality (for example: Pakistani versus Turkish), has led to a sense of marginalization even among the immigrants themselves. This makes for a fertile ground for jihadist recruitment, and many 'lone wolf' terrorists in the West have been found to have a petty criminal background. De-radicalization programs offer little protection against them because criminal-jihadists, unlike idealistic volunteers for jihad who do not know the realities of combat, are morally hardened.

Homeland security threat
Although the terrorist threat to Europe is miniscule in absolute terms, it still has the capacity to undermine inter-religious relations within European societies. For some years now,

Origins of foreign fighters in Syria

Number of foreign fighters, per million people   ▢ 0–20   ▢ 21–40   ▢ 41+
➡ Absolute numbers of foreign fighters (latest numbers as of mid-2014)

Sources: International Center for the Study of Radicalisation; Soufan Group; The Economist; Radio Free Europe

there has been a slow drumbeat of 'lone wolf' attacks, which gathered pace during 2014. From the May 2014 shooting at the Jewish Museum of Belgium to the *Charlie Hebdo* attack, lone wolves and 'amateur jihadists' (those who have received some para-military training, but operate on their own initiative) have demonstrated an astute political sense in their targeting

pattern. They have hit locations that have a high symbolic value but are relatively easy to access, thus requiring little preparation for an assault. They have fed into larger currents in the domestic politics of many European states – such as France, Norway and the United Kingdom – which see multiculturalism and immigrant assimilation as failed experiments. Hence, they have lit a spark that could in future years develop into a serious domestic security threat to Europe.

Even more worrying, lone wolves and amateur jihadists have had the effect of splitting policy attention between homeland security and combating large-scale terrorism overseas. With much of the media transfixed by *Charlie Hebdo* attack, little attention was paid to the near-simultaneous massacre of approximately 2000 people in northeast Nigeria. Through this massacre, Boko Haram consolidated its hold over Borno province and came a step closer to emulating the territorial dominance of the IS in Iraq and Syria. The group is now thought to have a strong presence in as much as 20 per cent of Nigeria's territory – an area the size of Switzerland. Meanwhile, in Mali, jihadists who had previously been routed by the French air and ground offensive in 2013 are quietly returning. Among their first initiatives upon recapturing territory is to

identify and eliminate all 'collaborators' who assisted the French. There is little that can be done to resist this trend, due to policy preoccupation with security threats closer home.

Much speculation has surrounded the question of foreign fighters travelling to join the IS. The number of EU nationals fighting with the group is estimated at anywhere between 3000 and 5000. Roughly 1200 come from France, home to Europe's largest Muslim and Jewish populations and thus considered a prime target for any spillover of violence from the Middle East. With Muslims representing eight per cent of the French population, but constituting around 70 per cent of all imprisoned criminals, jihadist recruiters have a simmering pool of resentment to tap into. Among political analysts, questions are being raised about whether the French effort to integrate marginalized communities is too much or too little. The answer to this would also be pertinent for Belgium, Denmark, and the UK, all of which have been heavily affected by IS recruitment campaigns. The group has revolutionized online radicalization, through a smart propaganda campaign backed up by money power and technical expertise.

To begin with, the IS gives great emphasis on relaying the positive

impressions of its rank-and-file recruits. This is in contrast to al-Qaida, which mostly allowed senior commanders to appear in its media releases and had them deliver drab, politically-loaded rants. IS members, on the other hand, narrate how life in the IS is appealing at a mundane level and talk about how civic services are provided to ensure a high standard of living. Although the truth is vastly different, impressionable and psychologically dislocated youth from around the world find the IS fantasy a tempting one. Although many join the group with the express purpose of waging violent jihad, a sizeable minority seem to actually believe that the IS represents a new experiment in state-building and wish to contribute to it out of pseudo-altruistic motives. Certainly, the Syrian civil war provides a cause to rally around, given the fierce repression practiced by the Damascus regime.

To avoid disillusioning its more idealistic supporters, the IS ensures that public disgust with its extra-judicial executions, including the beheading of Western journalists, does not swell into a counter-movement. Some beheading videos have been edited to leave out the goriest footage, thus presenting an illusion of a 'suffering-free' death. Those who are ideologically attracted to the IS model of politics find such killings morally palatable, since

they do not have to confront the human tragedy that is inherent in the act. At the same time, such footage, together with photographs of prisoner executions in official IS publications, exerts a psychologically strong pull upon viewers. Al-Qaida, forced to remain a de-territorialized group whose members are on most-wanted lists, lacks the resources, time, and space to match the sophistication of IS propaganda.

European security experts are sure that the influx of foreign fighters to the IS is a potential long-term problem. What they are not clear about is how this problem will manifest itself. The worst-case scenario – that of European jihadists returning home to create mayhem – is not assessed as very likely. This is because surveillance technologies introduced over the past decade have given law enforcement agencies a fairly good picture of their activities once they re-enter Europe. Only resource constraints and legal barriers (in some cases) prevent detailed case-specific knowledge of the public risk that each individual poses – both problems are unavoidable in free societies that do not wish to become police states. Instead of carrying out attacks themselves, such jihadist veterans might find it easier to serve as motivators, exploiting freedom of expression laws to inspire future

generations towards radicalism and if incarcerated, to win over prison inmates. This is a more insidious challenge, as Dutch investigators have discovered. Despite initial successes in scaring off aspiring jihadists from pursuing their plans, authorities have noted that in recent years, potential terrorists have learned how to game the system. The latter are now aware of their legal rights, and the limits of police power to intercept and question them. Consequently, they are becoming better at disguising their activities and staying below the surveillance grid. The most likely attack scenario would be one of 'amateur' terrorists, with a strong criminal background, carrying out operations based on logistics support obtained through gang contacts. While these preoccupy the attention of European security officials, Islamist insurgencies in the Middle East, North Africa, and possibly South Asia will likely make a determined grab for political power.

The IS is the key to the unfolding trend. As the primary pillar of jihadist resurgence since the death of Osama bin Laden and the Arab Revolts of 2011, its fate will closely shape other groups' enthusiasm for 'territorial' jihad. Meanwhile, al-Qaida and its affiliates are seeking to assert their continued relevance by encouraging attacks on Western homelands. Here, the third pillar – lone wolves and amateur jihadists – becomes crucial. It gives al-Qaida a strike capability which the IS might be compelled to acquire as well, once its cadres in Iraq and Syria are sufficiently demoralized by military setbacks against coalition forces. In such a situation, they will need fresh doses of courage injected into them through long-distance attacks in Europe, North America, or Australia. The fourth pillar – organized criminal activity – would serve as an enabler of such attacks, both financially and logistically, and in certain cases by providing additional manpower from the prison population of European states. Taken together, these four pillars of radicalism suggest that whatever the outcome of the campaign against the IS in the Middle East, Europe needs to remain vigilant. ●

CHAPTER 4

Vulnerable frontier: militarized competition in outer space

Michael Haas

Critical dependencies on space-based infrastructure have grown dramatically in recent decades, and now extend to small states and the global economy as a whole. However, as geopolitical rivalries re-emerge in more traditional domains of interstate conflict, the prospects for future stability in space appear increasingly dim. While the consequences of a great-power clash in space could be ruinous, a shared understanding of the perils involved has yet to take hold. Strategic interaction along the 'final frontier' is set to enter a period of considerable danger.

An SM-3 interceptor modified for the anti-satellite mission is launched from the guided-missile cruiser USS *Lake Erie* during *Operation Burnt Frost,* 20 February 2008.
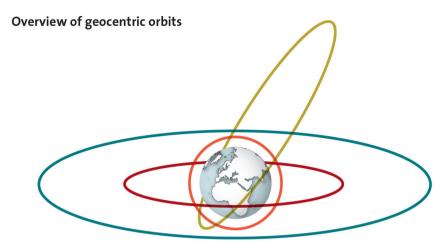
Among the various environments into which humans have expanded their economic, military, and scientific activities, outer space is easily the most unwelcoming and inhospitable. Impossible to access except through massive expenditures of energy per unit of mass to be placed into orbit, and utterly hostile to human life as well as to many types of man-made machinery, the maintenance of a permanent presence outside Earth's protective atmosphere remains a highly ambitious undertaking. Despite various complications, however, this presence – which, in most cases, has entailed the placement of unmanned artificial satellites in earth-centric orbits – has become an essential pillar of the global economic and security systems in the late 20th and early 21st centuries. From highly specialized scientific and commercial services to everyday applications of information technology (IT), space-based infrastructures now form part of the life-support system of a civilization that has tied its economic well-being and, indeed, its very survival to global connectivity.

However, while the economically most developed societies in particular have come to accept this state of dependence on space-based systems as fairly natural and unproblematic, the space domain is, in fact, highly vulnerable to the direct and indirect effects of reckless behavior on the part of both commercial and governmental entities. Instances of overcrowding are already in evidence within certain orbital planes, increasing the likelihood of serious accidents, such as the 2009 collision between the Iridium 33 and Cosmos-2251 communications satellites in low-earth orbit. Decades of ill-regulated activities in space have created millions of pieces of orbital debris, many of which have sufficient kinetic energy to permanently disable a satellite.

However, the most serious threat to the continued accessibility of the space environment by far is the prospect of a military confrontation, involving the use of kinetic anti-satellite (ASAT) weaponry by any of the growing number of states that now possess the technological wherewithal to field such capabilities.

As was rather vividly demonstrated by the Chinese test of a direct-ascent ASAT missile in January 2007, which is estimated to have created more than two million pieces of debris up to ten centimeters in size as well as 2,500 larger objects that can be routinely tracked by earth-based sensors, such a conflict would probably result in massive environmental damage. Depending on the number and position of satellites destroyed, the utilization of

Overview of geocentric orbits

- ● LEO = Low Earth Orbit (≈ 200 – 2,000 km)
- ● MEO = Medium Earth Orbit (≈ 2,000 – 35,000 km)
- ● GEO = Geostationary Orbit (≈ 36,000 km)
- ● HEO = Highly Elliptical Orbit (≈ 200 – 50,000 km)

Source: NASA Global Change Master Directory

affected orbital planes could be severely impaired. In a worst-case scenario, these orbits could become virtually unusable for extended periods of time, as most of the debris would remain in place for decades or even centuries, with serious implications for both commercial and military users.

Unfortunately, several trends point in the direction of an increased risk over the next 10 – 20 years of terrestrial conflict that may involve attacks on space systems, including the use of kinetic ASAT weaponry. These trends are primarily the results of the re-emergence of sustained strategic rivalries among some great and medium-sized powers – including the US and China in East Asia, the US and Russia in Eurasia, and potentially the China-India-Pakistan triangle in South Asia. With the exception of Pakistan, all of these states have already demonstrated a basic anti-satellite capability, and the US and China in particular are integrating space warfare scenarios into their military planning.

Moreover, the ongoing diffusion of underlying clusters of technologies – which include ballistic missiles and space launch vehicles (SLVs), advanced radar and seeker technologies, conventional and micro-satellites, solid-state or chemical lasers, as well

as battle management networks to co-ordinate attacks – will further increase the number of states with a latent anti-satellite potential. It is entirely possible that the pace of technology diffusion will accelerate further in the coming decades.
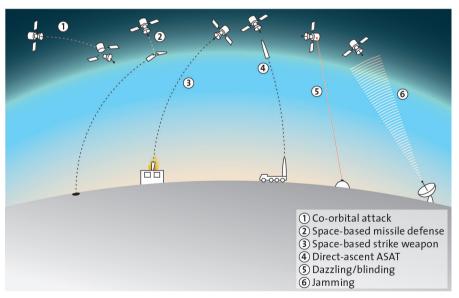
Against this backdrop of renewed strategic rivalry and continuing proliferation, the specter of space conflict will be a prominent feature of global politics in the coming decade and probably beyond. This chapter will first discuss the problematic, but largely irresolvable entanglement between civil and military activities in space, as well as the limited effectiveness of

multilateral governance instruments in regulating these activities. It will then outline in considerable detail the current geostrategic and military trends that increase the likelihood of military confrontations and render space an ever more vulnerable domain. Finally, it will review several ways in which states can mitigate their dependence on vulnerable space systems and provide an assessment of their potential effectiveness.

Irresolvable entanglements

Over the last several decades, space-based services have become a critical component of the global economic system as well as of the civilian

Space and ASAT weapons

1. Co-orbital attack
2. Space-based missile defense
3. Space-based strike weapon
4. Direct-ascent ASAT
5. Dazzling/blinding
6. Jamming

infrastructure of government. Long-range communications, public and commercial broadcasting, imaging and remote sensing, positioning and navigation, meteorology, and a host of specialized scientific applications are all highly dependent on the smooth functioning of satellites and their diverse payloads. Vital sectors of the globalized economy, including finance, shipping, and civil aviation, rely on these space-based infrastructures, as do agricultural planning, urban planning and surveying, disaster management, and environmental monitoring.

The provision of these various services is valued at over USD 300 billion per year, and has remained a growth industry even in the aftermath of the 2007–2008 financial crisis. The overall economic contribution of space-based infrastructure in terms of establishing global connectivity, reducing transaction costs, and providing unique sources of information about terrestrial activities is much more difficult to quantify. However, it undoubtedly makes a substantial contribution to the current gross world product of more than USD 74 trillion and thus likely exceeds the direct profits garnered by space-related industries many times over.

While space activities are still primarily conducted by a small number of advanced nations and private entities, the number of stakeholders has grown exponentially over the past 50 years. In its early stages, the utilization of space was the exclusive domain of the Cold War era superpowers. Today, only half of the more than 1,200 active satellites are still operated by the US or Russia, and in the case of the US almost half of those are owned by private businesses. Overall, more than 50 nations now have one or more satellites operating under their flag.

While the direct stakes of the leading spacefaring nations still exceed those of less capable or newly emerging actors, small states that are tightly integrated into the global economy are now nearly as vulnerable to disruptions of the orbital environment as are the great powers. At the same time, the capacity of most of these actors to unilaterally hedge against a loss of services without incurring unacceptable economic costs is rather limited.

This state of vulnerability, which is a product of states' dependence on space-based services and the current lack of viable alternatives to such services, is compounded by the fact that the infrastructures in question are inherently fragile. Due to the difficulty of placing them in orbit and keeping them in working order in the stringent conditions of the space

environment, space assets tend to be expensive, scarce, and difficult to replace. As a result of constraints in weight and size, they also typically lack physical robustness beyond what is absolutely necessary to keep them operational over their specified lifecycle. Consequently, the human foothold in the space domain is fundamentally less resilient than is our hold over other more easily accessible components of the global system, such as the maritime domain.

The situation is further complicated by the fact that any distinction between the civil and military spheres of space activity is at best porous, and in many cases non-existent. Not only are most space programs military in origin, they also tend to embody the very essence of dual-use technology, as their civil components are either direct corollaries of military services (as is the case with the US Global Positioning System, or GPS) or can be employed for military purposes with no, or only minimal, modifications (which is the case in many commercial communication and imaging applications). In fact, among some 500 satellites that are not directly related to a governmental or military agency, a substantial majority provide services that potentially have military applicability. As a result, debates about the perils of 'militarization' are largely moot – space is, and

has been ever since the 1950s, a thoroughly militarized domain.

This entanglement of civil and military infrastructures in space has important implications as far as future security dynamics are concerned. On the one hand, in case of a serious confrontation, their potential military relevance may require that a large number of foreign-operated spacecraft be considered as targets. Otherwise, an opponent would be allowed to immunize essential services from attack by outsourcing them to commercial entities or third parties. On the other hand, attacks on such third-party satellites would likely be perceived as particularly escalatory, requiring that fragile and ambiguous distinctions be upheld during a crisis or conflict. This would seem to create considerable opportunity for miscalculation and miscommunication.

At the same time, entanglement also accentuates the fact that civil and military infrastructures are equally vulnerable to any large-scale environmental effects of kinetic space warfare. Even if distinctions between enemy and 'neutral', as well as between military and commercial, spacecraft could be upheld, attacks would inexorably entail some amount of collateral damage within that particular orbital plane. While some military satellites are

already designed to weather specific types of adversarial effects, such as the electromagnetic pulse (EMP) created by high-altitude nuclear explosions, and could perhaps be better protected against other effects as well, a comprehensive program of satellite hardening would almost certainly entail prohibitive costs. Therefore, the prevention of destructive anti-satellite warfare would seem to constitute the only viable course of action if major risks to the existing infrastructures are to be avoided.

The hollow promise of comprehensive governance

Among the options available to policy-makers to ensure that space does not become the scene of serious military confrontation, the institution of a framework of binding rules and norms that underwrite the status of space as a non-weaponized 'sanctuary' that is off-limits to any direct military interventions would seem to hold considerable appeal. If such a framework were embraced and collectively upheld by all the relevant space powers, the possibility of space conflict would almost certainly diminish, and access to the space environment would continue to be relatively unproblematic for decades to come. In fact, several initiatives with the declared goal of achieving such an end state are currently on the table, including a draft treaty proposed by Russia and China in 2008,

which has recently been updated, and a non-binding code of conduct supported by the EU.

Unfortunately, hopes for a comprehensive scheme of governance that ensures the military inviolability of the space domain are largely based on extravagant extrapolations from the limited achievements of Cold War space diplomacy, or of more recent civil-commercial governance instruments. While the former were made possible by a specific set of political-military conditions that no longer apply, the latter fail to provide a workable template for regulating military activities in space, which are among the most sensitive and least transparent aspects in the military policies of the great powers. As a result, it is unlikely that multilateral governance will be able to effectively prevent terrestrial rivalries from spilling over into space. Far from offering any decisive solutions, it should be regarded as one of a number of mechanisms that may be able to make a limited contribution to a stable space environment.

Historically, space governance has enjoyed some success only where the great powers had a shared interest in preventing a further escalation of ongoing activities, notably where weaponization in the very narrow sense of permanently deploying specific types

of weapons in orbit, was concerned. This was laid down in the 1967 Outer Space Treaty, which remains to this day the most significant legal document regulating activities in space, and the now defunct Anti-Ballistic Missile (ABM) Treaty, ratified in 1972. While such partial achievements remain a possibility, trust in comprehensive multilateral governance would appear to be largely misplaced where military competition is perceived by one or both sides as providing important strategic or political advantages.

To the extent that effective governance remains elusive, space will once again become – and likely remain – a contested zone of influence, and potentially a zone of conflict, between the great powers. Governance efforts, in the form of confidence-building measures and arms control initiatives, could be instrumental in regulating the more escalatory or destabilizing aspects of militarized competition. The stationing of weapons in orbit, in particular, will remain a distinct and perhaps more manageable concern. That said, the re-emergence of strategic rivalries between several of the great powers and the persistence of rivalry in other settings indicate a heightening of competition in the near- and medium-term that any existing or proposed mechanisms of governance are unlikely to prevent.

The return of strategic rivalry and the rise of space denial

As the unrivalled military and economic predominance of the US, which has been the hallmark of the post-Cold War era, begins to wane, geopolitical competition with China in the Asia-Pacific and with Russia in Eurasia is inaugurating a new era of rivalry in an increasingly multipolar global system. Intermittent tensions in the East and South China Seas, which from a US perspective largely amount to confrontations by proxy over the future regional order, and the acute crisis in NATO-Russia relations over Ukraine are but the most visible crystallization points of these growing fault lines in great power relations. As scenarios of conventional or 'hybrid' interstate warfare begin to reshape the horizon of military planning, these rivalries are also increasingly finding their expression in outer space. But the strategic conditions under which the next round of militarized interaction in space will take place differ very considerably from those of the Cold War competition, and in ways that indicate a much greater potential for conflict escalation.

Of course, space has been an arena of geostrategic antagonism and jostling from the very inception of human orbital activities. Throughout the first half of the period since 1957, when

the civil and military utilization of space began in earnest, great-power relations were dominated by an entrenched militarized rivalry between two largely incompatible systems of government. However, alone among the environments into which humans have extended their economic and military reach, space has never seen a direct military clash between hostile political actors. This outcome might be seen as an encouraging sign of the great powers' ability to regulate their interactions even in the absence of comprehensive space governance or, at the very least, to successfully 'muddle through'. It appears increasingly unlikely, however, that this run of good fortune will hold indefinitely.
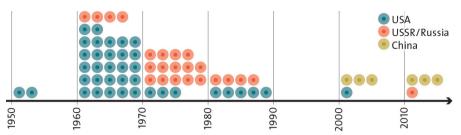
A strong case can be made to the effect that space conflict during the Cold War was of limited importance because it was viewed almost exclusively through the prism of space systems' intimate association with the strategic nuclear balance. Throughout the bipolar standoff, satellites were utilized mainly for strategic command and control (C2), early warning, and reconnaissance. As a result of this close integration of space and the nuclear sphere, attacks on spacecraft were generally seen as a corollary of, or prelude to, full-scale nuclear war, and considerably less attention was paid to space warfare as a serious issue during more

limited conflicts. It was thus expected that, should attacks on spacecraft ever occur, they would almost immediately be eclipsed by far more serious events.

It was only during the 1991 Gulf War that the current paradigm of space operations in support of conventional force deployments began to take hold. In the quarter-century that followed, the contribution of space-based services to conventional military operations has increased to the point of becoming the chief *raison d'être* of space power, with other advanced military forces clearly seeking to emulate the US in this regard. As a result of these developments, the perspective of potential ASAT users on space denial operations has changed completely. Far from being a prelude to an all-out nuclear assault, space warfare is now seen primarily as a means of denying information support and C2 to the opponent's conventional forces, thereby depriving them of vital force multipliers. Such considerations are particularly prominent in the warfighting concepts of armed forces that view the highly space-enabled and space-dependent US military as a likely opponent.

As a matter of fact, concerns about US conventional military superiority have been the main driver behind the

Kinetic ASAT testing

Sources: Brian Weeden (2014), *Through a Glass, Darkly: Chinese, American, and Russian Anti-satellite Testing in Space,* Broomfield, CO: Secure World Foundation; Michael Krepon & Julia Thompson (eds.) (2013), *Anti-satellite Weapons, Deterrence and Sino-American Space Relations,* Washington, DC: Stimson Center.

renewed interest in anti-satellite capabilities. Attempts at offsetting the US advantage in space – and thereby diminishing the US armed forces' overall margin of superiority in a future conflict – are now quite prominent in Chinese and Russian conceptions of future warfare, and are manifesting themselves in a number of development programs and tests not seen since the 1980s. With space warfare gaining currency in the doctrinal debates of some of the world's most capable armed forces, other nations are beginning to take an interest in military counter-space options as well.

The remarkable rebirth of ASAT

In retrospect, the developments that placed space warfare back on the agenda of great power politics were the direction taken by the Chinese People's Liberation Army (PLA) in its modernization drive, which finally began to gather some steam in the early 2000s, and the US decision in 2002

to withdraw from the ABM Treaty. It was only in the aftermath of China's much-noted shoot-down of its Fengyun-1C weather satellite in early 2007, however, that the issue began to reenter the public consciousness. It was this rather dramatic event, which drew a thinly-veiled US riposte in the destruction of the defunct USA-193 reconnaissance satellite in an ASAT test known as *Operation Burnt Frost* in February 2008, which reestablished the prospect of space warfare as a prominent global security concern.

In the eight years that have passed since the Fengyung intercept, a wealth of evidence has emerged that points to renewed efforts by several of the great powers to develop a capacity for effective space denial by both kinetic and non-kinetic means. Of these, China's development of the direct-ascent missile system, known as the SC-19, which was first observed in two non-destructive tests in 2005

and 2006, and also employed in the 2007 destructive test, has understandably received the greatest amount of public attention. Four additional tests with a suspected ASAT background have been reported in 2010, 2013, and most recently in July 2014. According to one notable technical analysis, one of two tests observed in 2013 may have utilized a more advanced missile and reached much deeper into space than did earlier tests, with an apogee in excess of 10,000 kilometers. The same may have been true of the test reported in 2014. Should the PLA be able to consolidate such an extended-range capability, it will be able to threaten a much greater number of satellites than has hitherto been the case.

One significant feature of the SC-19 system is that it has been tested in a road-mobile configuration, which points to the development of an operationally credible and survivable capability that may already be deployed in small numbers with the Second Artillery Force (SAF), which also has responsibility for the land-based component of China's nuclear deterrent. Even a few SC-19s could do considerable damage to selected high-value military assets in low-earth orbits, and the same could be true of the extended-range system purportedly tested in 2013 and 2014 if it is targeted against relatively vulnerable constellations in geostationary orbits. Meanwhile, the GPS constellation in medium-earth orbits is generally considered relatively robust, due to its distributed nature. Bringing the system to its knees for an extended period of time would require the coordinated expenditure of perhaps a dozen or more weapons, which would almost certainly draw an extremely robust – possibly nuclear – response from the US.

In addition to its direct-ascent, hit-to-kill system (or systems), China is also reported to be testing systems for co-orbital attack. This is based on the observation of a number of unusual maneuvers by satellites Shiyan-7, Shijian-15, and Chuangxin-3, which are thought to have begun in July 2013. The exact extent and implications of this additional path to an ASAT capability are currently difficult to fathom. Moreover, the PLA is known to also have engaged in the 'dazzling' or 'blinding' of US imaging satellites by means of terrestrial laser systems, and has likely acquired GPS jammers, which can be effective in protecting critical installations from certain types of precision-guided munitions (PGM). It may also be developing a range of other space warfare techniques based on microwave, electronic attack, and cyberspace capabilities. Given the considerable breadth and depth of its space warfare programs, the PLA's

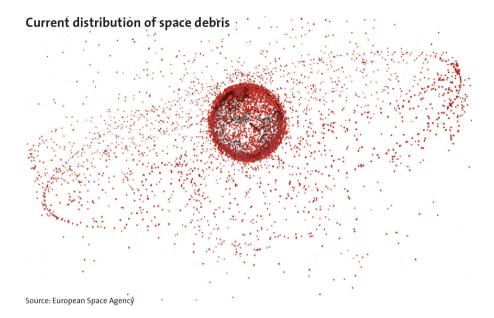activities are currently the main driver of a burgeoning arms dynamic in this area of strategic interaction.

The US, meanwhile, is not known to be operating or developing dedicated anti-satellite weapons, which is explained in part by the much lower dependence on space-based services of even the most capable among its potential opponents. The US military does, however, field several types of missile defense interceptors, some of which are inherently dual-use capable, as was successfully demonstrated in *Operation Burnt Frost*. Its ballistic missile defense (BMD) programs thus provide the US with what is probably the most extensive and most widely distributed ASAT potential among the great powers. However, the reach of this arsenal is currently limited to low Earth orbits. Moreover, while the BMD and anti-satellite missions are fundamentally very similar, and satellites are much less operationally demanding targets, substantial technical modifications are nonetheless required to realize the latent ASAT potential of these systems. It is therefore fair to say that the US does not routinely field space weapons as part of its global defense strategy.

The Russian Federation is also reportedly engaging in a variety of space warfare activities, driven in large part by US insistence on a continental missile defense system, which Moscow perceives as a potential threat to its nuclear deterrent, as well as by Chinese and US ASAT testing. The most recent example of such activities is what may amount to a reactivation of the co-orbital attack programs that constituted the backbone of Soviet space warfare during the Cold War. According to media reports, a satellite launched in May 2014 and known as Cosmos-2499 has been engaging in unusual approach maneuvers that may constitute a series of ASAT-related tests. Russia has also maintained and recently updated the ground-based sensors that used to support its co-orbital attack programs. In addition to its traditional focus on co-orbital attack, Russia may be reviving its air-launched Kontakt system as well as an airborne laser that could be employed to temporarily dazzle, and perhaps even permanently disable, satellites in low Earth orbit. Russia is also a leading manufacturer of GPS jammers, which it has exported to various countries.

Another significant military power that is known to possess at least a latent direct-ascent ASAT program is India. The Indian armed forces are currently working towards a layered missile defense system and have so far conducted at least seven tests, which may have provided sufficient know-how to conduct an ASAT mission

Current distribution of space debris
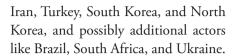

Source: European Space Agency

with relative ease. India is not currently known to be developing or fielding a dedicated capability, but is sure to keep a close watch on China's activities in this area, given its own growing stakes in outer space, its unresolved territorial disputes with that country, and a potential for serious geostrategic competition in the Indian Ocean.

Other nations that currently possess the technical prerequisites for direct-ascent or co-orbital attack systems and could field such systems within years of a political decision to do so include Japan, Israel, and France. In fact, Japan's deep involvement in the Aegis BMD program means that it is already in possession of a latent capability

similar to that of the US. France and Israel are both nuclear powers with considerable military stakes in space, although it would appear that neither is critically dependent on space-based C2 or early warning for the integrity of its deterrent. However, even in the absence of such dependence, these states may come to decide that an ASAT capability of some kind is desirable for symmetrical deterrence of threats to their spacecraft. In addition to these established space powers, the proliferation of satellite, launch system, and precision-guidance technologies means that a growing number of states will possess latent space warfare capabilities in the future. They will most likely include Pakistan,

Iran, Turkey, South Korea, and North Korea, and possibly additional actors like Brazil, South Africa, and Ukraine.

ASAT and counter-ASAT in great-power military planning

While a number of actors possess mobilized or latent ASAT potentials, only the US, China, and the Russian Federation are known to be integrating these potentials, or military options of dealing with enemy potentials, into their war planning. While Russian doctrinal statements have generally focused on the threat posed by opponents' space warfare capabilities to its own strategic warning and C2 assets as well as on the possibility of deploying ASAT weaponry against the space-based elements of a US ballistic missile defense system, many more details are known about the emerging Sino-American interactions in this area.

From a Chinese perspective, space warfare is perceived as a critical element of a 'counter-intervention' or peripheral defense strategy designed to deny US military forces access to China's immediate maritime environment in event of a conflict over Taiwan or other vital Chinese interests. Given the PLA's sustained investment in this strategy, the creation of such an exclusion zone is now no longer an idle threat, even though serious deficits are thought to persist in areas including

joint operations and operational command and control. Chinese planners view US space assets as important enablers of US military superiority, and being both vital and vulnerable, they are seen as highly attractive and, indeed, natural targets for any serious anti-access strategy.

As a result, the PLA is preparing to target US satellites at the outset of a conflict to partially equalize what is still a seriously skewed balance of military power in the Asia-Pacific region. One must assume that PLA planners are aware of the escalatory implications of any such move, but it appears that this has not led them to rule out such a course of action, which could provide substantial advantages once war initiation is perceived as inevitable. It is, however, likely that the PLA would seek to keep the use of kinetic weaponry to an unavoidable minimum, to forestall unnecessary escalation as well as excessive international opprobrium, and perhaps to retain this most extreme option as part of a strategy of intra-war deterrence. This is particularly likely as non-kinetic alternatives including electronic attacks, cyber-attacks, and reversible laser or microwave attacks may be available in many cases. One can also expect that Chinese reluctance to escalate immediately to a kinetic exchange would increase further as the

PLA itself becomes more dependent on space-based services as well.

It is much less clear, however, that artificial 'firebreaks' instituted and tacitly or explicitly communicated at the outset of a conflict would hold as US and Chinese forces engage in high-intensity, conventional exchanges, suffering grievous losses and progressive disruption of essential services and capabilities. It is also unclear whether space systems employed in support of conventional forces can be distinguished from systems that are entangled in the strategic nuclear deterrent with sufficient clarity to avoid, at a minimum, the impression of a coordinated and sustained attack on the opponent's nuclear forces. In some cases, including infrared sensors deployed for early warning, which would likely also be employed to locate conventional missile batteries, this would be next to impossible. Overall, even a Chinese strategy of highly selective space warfare could trigger escalation to the nuclear level.

Such a dynamic could be compounded by current US military planning, which also exhibits some highly offensive traits and which must contend with the inherent vulnerability of vital assets. Given the tense fiscal environment and the timelines for fielding new and more survivable platforms

or advanced payloads, this state of affairs may well persist into the 2030s. To offset the current vulnerability of the nation's military posture, planners may opt to counter or even preempt Chinese initiatives with early attacks of their own that would have to be directed against some of the most threatening capabilities and installations, which would generally be situated on the Chinese mainland.

One of the more worrisome aspects of the US doctrinal debate is the suggestion, which has gained some traction in recent years, of using conventional prompt strike weaponry to disable the PLA's most threatening ASAT systems before they can be brought to bear against vulnerable US satellites. While such attack options are not currently available, the reliance on missile-based prompt strike during the early hours of a conflict would further compress decision-making timelines and create 'use-or-lose' dilemmas on both sides of the equation. The implications of such developments for crisis management and conventional first-strike stability could be grave, and cross-domain linkages including to cyberspace and the nuclear sphere are sure to complicate political and military decision-making even further.

On the other hand, the development of viable alternatives to space-based

services and of doctrinal constructs for operations in space-denied environments could serve to reduce the incentives for early attacks on space or counter-space systems on both sides of the confrontation. Hence, the current vulnerability of space-based services might provide sufficient impetus for change to avoid some of the more destabilizing implications of the renewed interest in the means and methods of space warfare, and may eventually lead to closer consultation between the great powers.

Robust deterrence or fragile state of non-aggression?

Ultimately, however, the avoidance of the more destructive forms of space warfare would seem to require not just the successful management of successive crises as they emerge, but ultimately the institution of stable deterrence relationships between the main parties to this burgeoning competition. This will depend in part on the effective communication of deterrent threats, based both on denial (the ability to negate the opponent's initiatives, for example by creating sufficient redundancies and being able to operate effectively even in the absence of space support) as well as punishment (the ability to impose unacceptable cost by inflicting symmetrical or asymmetrical damage).

Even more than on these well-known elements of a credible deterrent strategy,

the prevention of space conflict may depend on the recognition of mutual vulnerability in space, and the internalization of a sense of shared interest in avoiding worst-case outcomes. While there are obvious similarities to the nuclear sphere, the situation with regard to the space environment is complicated by several factors.

First, the consequences of a kinetic exchange in space are not very well understood, and the proposition that catastrophic damage to orbital infrastructures would be the most likely outcome of such an exchange is not universally accepted. Consequently, the exact degree of vulnerability and the likely ramifications of a military clash remain a matter of debate. While few analysts would deny that unrestrained space warfare would entail serious collateral damage, the 'crystal ball effect' that is associated with nuclear weapons is not nearly as clear-cut with regard to space warfare. This raises the possibility that some decision-makers may calculate that the political aftershocks and economic costs of waging war in space will be commensurate with the advantages gained by crossing this threshold. The total absence or very low number of human casualties constitutes another fundamental difference between nuclear and space warfare, and may serve to underline such considerations.

Secondly, the availability of non-kinetic options and the possibility, at least in some scenarios and with some proposed technologies, of achieving kinetic effects while keeping environmental damage to a minimum would lower the initial threshold for attacks against space systems even further. While a space conflict, once joined, may still spiral out of control, resulting in massive damage to civil and well as military infrastructures, initial military steps may not suggest that such an outcome is likely. This would also tend to undermine any shared perceptions of vulnerability.

Finally, future technological developments may increase the actors' ability to reconstitute the space environment by removing some (though certainly not all) debris, increasing the robustness of space systems, or rendering them more easily replaceable. Such developments would also tend to make kinetic attacks a more palatable option. In addition, some types of debris removal capabilities may also have an inherent dual-use ASAT potential. The introduction of space-based strike weapons for use against terrestrial targets, which also remains a possibility, would add a further layer of complications.

While the case for mutual vulnerability in space can be overstated, none of the factors cited above change the fundamental fact that the human presence in space is comparatively fragile and will continue to be vulnerable to disruption as a result of military conflict. All of them, however, might make it more difficult to avoid such conflict in the long run. Overall, then, despite some striking similarities, deterrence relationships based on mutual vulnerability are bound to be significantly less robust in space than is the case in the nuclear field.

Managing vulnerability in the new era of rivalry

Fortunately, a number of options are nonetheless available for hedging against the ramifications of conflict, and many of these would also serve to render space warfare a less attractive course of action. A first line of effort would involve the supplementation or partial replacement of space-based systems with terrestrially based, airborne, or near-space systems for communication, positioning, and other critical applications. While this would not solve the basic problem of vulnerability in space, it would create redundancies, reduce the effectiveness of space denial programs, and serve to partially deflect the military competition from the space arena. States could also seek to reduce the reliance of their civilian and military activities on space-based assets wherever possible,

which would diminish – though certainly not eliminate – the impact of any future disruptions.

A second line of effort would rely on more technical approaches designed to mitigate particularly destabilizing aspects of militarized competition through targeted confidence- and security-building measures, and perhaps eventually more robust arms control agreements. A moratorium or ban on counter-space weapon testing would be extremely useful during the earlier stages of a competition, but may be difficult to achieve in practice. As is often the case in arms control processes, a slow, deliberate, and incremental approach may offer the greatest chances of success. While they would severely hamper vertical as well as horizontal proliferation, these measures would leave in place existing capabilities and would entail significant verification challenges. Non-proliferation measures, including more stringent export controls on dual-use goods and technologies, may (or may not) prevent

additional actors from entering into competition. Finally, increased space situational awareness would increase the risk of cheating on any existing or future agreements, especially if it were to be provided by a multilateral agency.
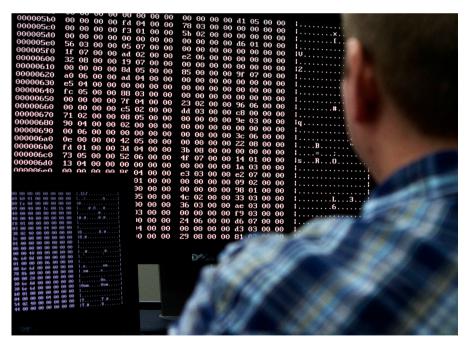
Despite the considerable potential of such targeted mitigation measures, the possibility that space may yet become the scene of military conflict will undoubtedly remain, and the essential fact of civil as well as military vulnerability is likely to persist well into the future. Given that a stable sense of mutual vulnerability is unlikely to emerge in the short run, and may not hold in the long run, the re-emergence of serious space rivalries is a cause for concern, both for established space powers and for small states that depend on space-based services provided by others. For better or worse, the coming decade may be decisive in shaping the future of our tenuous presence along this vulnerable frontier.

The normalization of cyber-international relations

Myriam Dunn Cavelty

> We have arrived in an age of mega-hacks, in which high-impact and high-attention cyberincidents are becoming the new normal. The increase in strategically consequential, targeted cyberincidents is met with intensified efforts to reduce the risk of cyberconflict through norm-building, mainly geared towards creating deterrent effects at the state level. While these new developments have an overall stabilizing effect on cyber-international relations, the narrow focus on destructive cyberattacks and on state-to-state relations is creating unintended security-reducing side-effects.

An analyst looks at code in the malware lab of a cyber security defense lab at the Idaho National Laboratory in Idaho Falls, Idaho, 29 September 2011.

For half a decade, cyberincidents, both big and small, have made the news almost daily. The fact that insecurity in and through the cyberdomain has come to dominate political discussions is not a trend – it is old news. Nevertheless, something has subtly changed in the last few years: There is an increasing sense of unease about the escalatory potential of cyberconflict, mainly fueled by the certainty that more and more states are using cyberspace to achieve strategic ends. As a result, the traditional world of states is more actively seeking to stabilize political interaction in and through cyberspace by a variety of means. Overall, cyberspace has been upgraded to a strategic domain whose development is no longer left to non-state actors.

This chapter focuses on the efforts of states to pacify cyberspace. It explores both, the causes of this trend as well as wanted and unwanted consequences of this gradual normalization of cyber-international relations. Despite big differences between traditional security problems and the newer issues of cyberspace, states are using traditional tools of diplomacy and statecraft, shaped and tested during the Cold War, to develop norms. On the one hand, this stands in contrast to two major truisms of our age: that states have no power in the virtual realm and that traditional state response strategies

are useless because the cyberdomain is too different. Since the cyberdomain is not a natural environment that develops beyond human control, it is almost entirely malleable. In other words, traditional response strategies and rules of conduct can be made to apply – at least in part. On the other hand, a focus on state-to-state relations and a focus on cyberattacks with destructive effects leaves two major issues untouched: first, how to extend norms, understood as shared expectations about appropriate behavior held by a community of actors, to non-state actors (both, as threat actors and security providers); and second, how to deal with large-scale cyberexploitation, or activities that are not destructive, but are used to extract data or to prepare for potential future 'cyberwar'. This omission leads to paradoxical effects: Even though more stability for state interaction is created, other state actions are, directly and indirectly, to blame for making both, the virtual but also, by implication, the real world rather less than more secure.

This chapter has three sections. The first discusses two developments in cyber-in-security. The first is about the 'normalization' of cyberconflict and the second about targeted attacks. Both trends give the impression that aggression in the virtual space has destabilizing effects and that there

is a high risk of escalation. A second section describes the attempts between states to stabilize interaction in cyberspace as a result of these insecurities and shows how norm-building is used to attempt cyberspecific deterrence. The third describes intended and unintended effects of these stabilization efforts, pointing to the main sources of tension. In conclusion, the chapter shows that the current stabilization and normalization processes are doomed to fail, unless the underlying issues are recognized and tackled.

Two trends in cyberaggression

To understand why states are seeking to stabilize cyber-international relations more actively nowadays, it is necessary to comprehend perceptions and realities of cyber-in-security. Two developments in cyberaggression stand out: The first is a shift in focus away from theoretical 'doomsday' cyberattack scenarios towards the reality of cyberaggression in conflict situations, which concerns both state and non-state actors. The reason for this shift is the 'normalization' of low-level cyberconflict as an add-on element to political disputes or conflicts. The second is a shift of attention from random occurrences to specifically targeted attacks. On the one hand, we have seen an increase in so-called 'mega-hacks' – successful data breaches in high-level economic or political targets. On the

other hand, the focus of the debate is now on so-called advanced persistent threats, APTs, malware that is quite sophisticated and often written for a specific purpose or target. Both, mega-hacks and APTs, are signs of the increasing maturity of aggression and the professionalization of attackers. In combination, they point to the increasing involvement of states in cyberaggression.

From theoretical doomsday scenarios to low-level cyberconflict

The two strategic key concerns with regards to cyberspace are low entry costs for disruptive 'cyberweapons' and the high vulnerability of critical infrastructures, which are increasingly dependent on cyberspace for a variety of information management, communications, and control functions. This dependency, and interdependency, has a strong national security component, since information infrastructure supports and enables crucial services for the functioning of economy, government, military, and society overall. As a result, for years, the greatest threat in the virtual realm, discussed in strategic circles, has been a deadly destructive cyberattack out of the blue that would bring a country to its knees within seconds.

Even though the term 'cyberwar' is still used frequently and

Low-level cyberconflict / cybermobilization

Incident	Description	Actors
Estonia (2007)	• 3 week long wave of Cyberattacks accompanying riots in Estonia sparked by the removal of a Red Army soldier statue	• Patriotic (pro-Russian) hackers • No proof of state involvement – but also failure/ unwillingness to stop the attacks
Georgia (2008)	• Cyberattacks accompanying five-day international military conflict between Georgia and Russia	• Russian Patriotic Hackers • Russian Business Network (Criminal Internet Service Provider) • No proof of state involvement, but also failure/ unwillingness to stop the attacks
Ukraine (2013–)	• Cyberattacks accompanying the Russo-Ukrainian crisis	• Cyber Berkut (and other pro-Ukrainian hacktivist group) • Russian Patriotic Hackers • Paid cyber trolls
North – South Korea (2013)	• Cyberattacks accompanying the heightened crisis	• The New Romanic Cyber Army / The Who Is Team (hacker groups, claimed responsibility • North Korea (?)
Gaza (2014)	• Cyberattacks accompanying 'Operation Protective Edge'	• Pro-Palestinian actors (Anonymous, Hamas, Syrian Electronic Army, Iran Cyber Army) • No proof of state involvement

indiscriminately for any kind of cyberaggression, and doomsday scenarios continue to be referenced both, in policy circles and in the media, the larger attention of most experts has shifted to the political and strategic implications of low-level cyberconflict or cybermobilization. This shift occurs as strategic cyberwar or cyberterrorism for that matter – understood as stand-alone, out-of-the-blue cyberattacks against civilian infrastructure – is considered highly unlikely among experts, due to practical and strategic reasons since it is very hard to control the effects of cyberweapons and make them last long enough to serve a long-term strategic purpose. In contrast, low-level cyberconflict – or cybermobilization – occurs as an

Methods	Targets	Impact
• Distributed Denial-of-Service (DDoS) attacks, using botnets • Website defacements (Russian propaganda)	• Websites of Parliament, Prime Minister and President • Websites of Foreign Ministry, Ministry of Justice • Estonian Daily newspaper and broadcasters • Hansabank	• Very low primary impact (Websites unavailable, economic damage • Huge secondary impact: has become a signature event to prove how dangerous cyberconflict is
• DDoS-attacks • Website defacements	• Websites of the President of Georgia • Georgian Governmental Websites • Georgian Newssites • Russian Newssites • Georgian Banks	• Very low direct impact, also because Georgia is not heavily dependent on IT-infrastructure • Another signature event for 'cyberwar'
• DDoS-attacks • Website defacements • Data dumps • Disinformation and propaganda campaigns • Disruptions and infiltration of internet and mobile phone traffic	• Government websites and prominent media outlets telecommunications • Internet traffic	• Low effect on the conflict itself
• DDoS-attacks • Malware that wipes master boot records • Defacement of websites	• South Korean banks and broadcasting companies	• Relatively low effect on long-standing conflict • Has heightened attention on North Korean cyber-capabilities
• DDoS-attacks on Israeli targets • Website defacement • Data dumps • Spear-phishing	• Israeli websites	• Very low effect on the conflict itself

add-on to 'normal' conflict or political disputes. It mainly consists of information dissemination activities and hacktivism, a portmanteau word that combines 'hacking' and 'activism', in which different actors try to manipulate the public infosphere or in which non-state actors side with one of the conflict parties use cyberspace for disruptive activities.

While strategic cyberwar is about (very) low-probability, (very) high-impact events, low-level cyberconflict is about medium- to high-probability, low- to medium-impact events. There have been no known instances of the first case, but many of the second.

These incidents demonstrate that it has become routine for non-state

actors to try and influence the larger infosphere before or during conflicts/disputes. Cyberspace facilitates the proliferation, and use, of capabilities needed for information campaigns, and no hacking skills are required to obtain and operate disruptive malware like Distributed Denial-of-Service (DDoS) tools for political ends. Events of this kind with the biggest impact are those like Estonia in 2007, in which state-involvement is suspected but relatively hard to prove, or Georgia in 2008, in which there were clear attempts to dominate the public infosphere. That said, easy-to-use tools for DDoS attacks, for example, which always gain much attention because they produce visible effects, have relatively little lasting effect on the overall conflict. In other words, this type of cyberaggression is defined by low barriers to entry but also low direct impact – unless we take into consideration the secondary, and often delayed, effects on the broader strategic-political context, which is fundamentally shaped by overblown reactions to relatively low-impact events, such as the attacks on Estonia.

Targeted attacks: hacktivist campaigns and APTs

The second development is a shift away in focus from cyberthreats that attempt to infect or affect as many machines as possible – as done by most viruses, botnet malware, or spam mail servers – towards smart targeted attacks that use tools to get specific information or to disrupt a specific system. What is causing this shift, is the professionalization of the cybercrime market and more state involvement in cyberexploitation activities. That said, this type of targeting behavior is not entirely new: The period between 2008 and 2012 was dominated by headlines about targeted hacktivism. During that time, the hacker collective Anonymous successfully engaged in politically motivated, digital vigilante campaigns either to humiliate high-visibility targets by DDoS attacks or to point out cases that constituted interferences with freedom of information and freedom of speech, often by making secret information available. In comparison to the hacktivism during times of conflict, this type selects targets depending on a feeling of collective anger or outrage without the context of a conflict.

The fact that this type of hacktivism is viewed through the lens of national security at all is due to the nature of some of the targets that were chosen. Financial institutions, which were targeted in Operation Payback in 2010, for example, are considered 'critical infrastructures' by all states, so that cyberattacks against them have to be taken seriously by security actors.

This also explains why incidents such as DDoS attacks, which are technically simple and harmless in terms of consequences, are often designated 'national security' issues. Furthermore, because some hacktivist campaigns aim to 'set information free', they clash with the state's prerogative to classify information and keep it secret. In 2011, hacktivist groups with higher technical proficiency went after high-level and security-designated targets such as the cybersecurity contractor HBGary Federal, the global intelligence company situated in the US Stratfor, or the CIA website. Several governments reacted with show trials of hackers and harshly prosecuted several of the individuals responsible for the above break-ins. Clear attribution was possible, due to an insider who helped the FBI and other security agencies to collect evidence against members of this group as part of a plea deal.

The steep decline in spectacular Anonymous-led hacktivist campaigns in recent years is likely due to the rather severe public punishment of misdeeds and a growing realization that cyberspace might not be quite as anonymous as assumed among hobby hackers. However, even though digital vigilantism and their showcase hacks have become less prominent, so-called 'Mega-Hacks' have exploded in numbers as it is shown in Figure 1. This
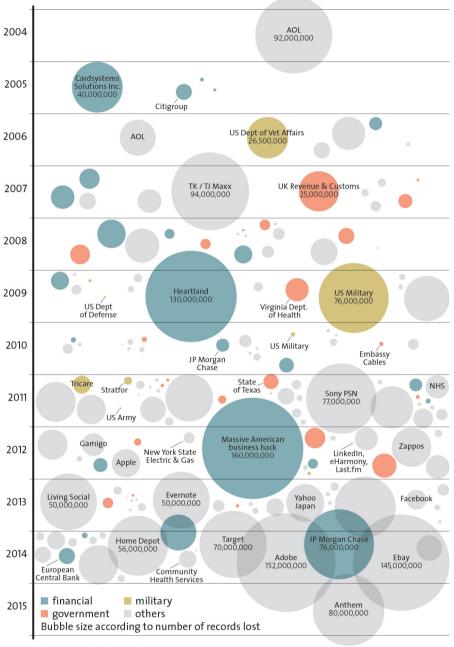
form of cybercrime focuses on stealing massive amounts of (badly) secured data, like costumer records, credit card information, or e-mails. Costs such as forensic expenses, fines, legal fees, re-organization, reputational damage, and class-action lawsuits exceeded USD 100 million in several cases. Breaches and data theft at Boeing, the US Transportation Command, the US Army Corps of Engineers, and the US Investigations Services once again established a clear link to national security.

The motivation behind these hacks seems to be mainly criminal, but some seem at least partially politically motivated, making a clear categorization difficult. In some cases, state-involvement is suspected, like in the recent Sony hack, which was attributed to North Korea by the FBI. However, most of the data breaches and subsequent data dumps do not require advanced hacking skills at all, which shows how poor the standards of information security in large parts of the economy and government are.

There are targeted attacks of a different league, however, called Advanced Persistent Threats, APTs. APTs are stealthy and continuous cyberoperations targeting a specific entity's information or functionality. They are advanced because the malware that is

Selected 'Mega-Hacks' since 2004

2004
AOL
92,000,000

2005
Cardsystems
Solutions Inc.
40,000,000
Citigroup

2006
AOL
US Dept of Vet Affairs
26,500,000

2007
TK / TJ Maxx
94,000,000
UK Revenue & Customs
25,000,000

2008

2009
US Dept
of Defense
Heartland
130,000,000
Virginia Dept.
of Health
US Military
76,000,000

2010
JP Morgan
Chase
US Military
Embassy
Cables

2011
Tricare
Stratfor
US Army
State
of Texas
Sony PSN
77,000,000
NHS

2012
Gamigo
Apple
New York State
Electric & Gas
Massive American
business hack
160,000,000
LinkedIn,
eHarmony,
Last.fm
Zappos

2013
Living Social
50,000,000
Evernote
50,000,000
Yahoo
Japan
Facebook

2014
European
Central Bank
Home Depot
56,000,000
Community
Health Services
Target
70,000,000
Adobe
152,000,000
JP Morgan Chase
76,000,000
Ebay
145,000,000

2015
Anthem
80,000,000

■ financial   ■ military
■ government   ■ others
Bubble size according to number of records lost

Sources: DataBreaches.net; IdTheftCentre; informationisbeautiful.net

used is sophisticated. They are persistent because there is constant monitoring of the activity of the malware and often constant extraction of data. And they are called 'threats', in line with information security vocabulary, since they are orchestrated by a human actor. Granted, the percentage of APTs in the overall malware environment is very small – a maximum of three per cent, according to some analysts – but due to their potentially considerable effects, they have gained a lot of attention in recent years.

Also, there is no question that APTs embody the involvement of states in cyberspace operations. While there are low barriers to entry for patriotic and activist hackers, the barriers to entry are substantially higher when it comes to cybertools used to achieve strategic objectives. To achieve controlled effect, it is necessary to have the capacity to know and then exploit the vulnerabilities, parts of the code that can be exploited, in specific systems around the world. Overall, the insecurity of the information infrastructure is endemic: So-called vulnerabilities abound, and many of them are either not (yet) known, are known just to a few, or are known, but nobody has an incentive to patch them. Depending on what can be done with them, some vulnerabilities have high strategic or monetary value and are sold for

as much as USD 200,000 to 300,000, often to national intelligence actors.

Once knowledge of an unpatched vulnerability has been gained, malware to exploit that vulnerability can be written. At minimum, this requires technical brainpower, labs that duplicate the target environment for testing, and a lot of time. In addition, many APTs are most likely inserted into the target systems by on-site personnel, including insiders. Most APTs remain undetected for years and gather large amounts of data during that time. Once malware has been inserted, it can also be modified in its behavior later; for example, to start deleting information or to tamper with other data functions. As a result, there are currently no good defenses against APTs. The usual tools like virus scanners and firewalls certainly do not work, but even air-gapped systems that are not connected to the internet can be infected, for example through a human agent.

Deterrence effects through international cybersecurity norms

The two cyber-in-security trends, normalization of low-level cyberconflict on the one hand and increasing state involvement on the other, demonstrate that the tools for and use of aggression have matured considerably in the last few years. The overall

feeling in many strategic circles, partially supported by statistics, is that the problem has gotten worse, both, in quantity as well as quality. Many experts call APTs cyberweapons and regard the build-up of capabilities by state actors as part of an arms race in cyberspace. The uncertainty about the intentions of other states and the practical inability to know whether such capabilities are used for offense or defense, lead to heightened feelings of insecurity and, in a classical security-dilemma fashion, to high incentives for building up (offensive) cyberwar capabilities and cybercommand units.

The further militarization of the virtual realm seems unstoppable at this point. However, the high feelings of insecurity have also led to higher incentives for states to control the risk of escalation and conflict. As a result, the number of ministerial meetings and conferences has increased substantially, and the first norms aiming to curb aggression in and through cyberspace are emerging. In this section, three types of developments are described that are leading to more stability in international relations through norm-building. The first concerns the establishment of transparency and confidence-building measures, TCBMs, for the use of information and communication technologies in

conflict. The second occurs in the field of international law, where rules of warfare in and through cyberspace are being established. The third is the attempt to make deterrence apply to cyberspace, which builds on both of the other developments.

Transparency and Confidence-Building Measures
The notion of Transparency and Confidence-Building Measures (TCBMs) in international relations emerged from attempts by the Cold War superpowers to lower the risk of nuclear war. Based on the experience that uncertainty about the intentions of a rival has great escalatory potential, these measures aimed to create more overall transparency, enhance the mechanisms for early warning and predictability of action by enhancing one's knowledge of the capabilities of the other and by institutionalizing lines and forms of communication.

In the virtual realm, there is a high risk of misperception and therefore escalation, mainly, because hostile actions are notoriously hard to attribute and because almost all 'cyberweapons' are of dual-use nature. Actions in cyberspace leave ample room for speculation as to underlying intentions and purposes, and it is easy for third parties to start false-flag operations to provoke a cyberconflict

that suits their interests. Since classical arms control initiatives based on regulating technical capacities do not work in this realm – cyberattacks rely on knowledge about computer code and organizational routines that cannot be prohibited and/or controlled at any sensible cost – the existing proposals for stabilizing this environment are about TCBMs, with a main focus on transparency measures.

After years of failed attempts to come to any kind of multilateral agreement, the Organization for Security and Co-operation in Europe, OSCE, managed to establish an 'Initial Set of OSCE CBMs to Reduce the Risks of Conflict Stemming from the Use of ICTs' in December 2013. The CBMs focus mainly on transparency measures to allow for exchange of information and communication on several levels, all voluntary. Granted, since no notification or observation measures are included in the OSCE agreement, it is little more than an expression of goodwill between participating states at the moment. However, the document has an important psychological effect in that it proves that consensus is at last possible in international cybersecurity. Furthermore, a second set of CBMs is being discussed. The existing agreement also serves as a platform for engaging other stakeholders, such as civil society, academia and the private sector.

At the same time, dialogs have been taking place between states and between states and other relevant stakeholders, all of them aimed at building better understanding, trust, and confidence between the parties and at establishing joint information mechanisms to avoid escalation to armed conflict. In sum, even though the results of these processes are a far cry from what would be needed to fully stabilize cyber-international relations, reaching even minor agreements in this area is a considerable step forward, given how ideological differences have acted as fundamental stumbling blocks for years.

The law of cyberwar

Beyond transparency and confidence building measures, the applicability of international law to the cyberdomain has been discussed for years. In 2013, finally, a consensus emerged among several states, and at the UN, in the EU, and in NATO, that International Humanitarian Law, IHL, fully applies in cyberoperations. In parallel, the applicability of state sovereignty and the international norms and principles that flow from sovereignty were also confirmed by several intergovernmental bodies. The most important questions with regard to *jus ad bellum*, i.e., when a cyberattack would be considered an armed attack by another state and how to

react in that case, are discussed in the influential 'Tallinn Manual on the International Law Applicable to Cyber Warfare', which was written by a group of international legal experts in a three-year consultation process and published in 2013.

The Tallinn Manual, which sets out 95 black-letter rules governing cyberconflicts, states that any cyberoperation by one state that causes meaningful damage or injuries to another can be considered an 'international armed conflict'. This is extended to non-state actors: an international armed conflict exists whenever a state is in 'overall control' of a group that launches a substantial cyberattack against another state. In most cases, therefore, IHL will apply to cyberoperations involving a non-state group only when the operations are one component of the group's traditional hostilities or take place under the direction of a state. Clearly, most hacktivist attacks do not fall under this definition because they do not create severe effects and because proving a link to the state is very difficult in many cases. Indeed, the biggest issue in this whole debate is whether a cyberattack could actually be attributed to the perpetrator with enough certainty to make the logic of 'armed attack' apply. Because of how information is transported through cyberspace and because of the potential time lag

between the effect of a 'cyberweapon' and the actual moment when such an APT is inserted into a network, there often is a serious attribution problem.

Making the logic of deterrence work
Attribution is also the biggest impediment against making traditional strategic concepts such as deterrence, especially deterrence by punishment, work. However, there are clear signs that the US is working systematically to build a specific deterrence regime for cyberspace, which encompasses both, deterrence by denial and deterrence by punishment. The considerable involvement of US officials in many of the international cybersecurity governance processes is linked to its strategic interest in shaping international norms for behavior in cyberspace, which will create more certainty about the costs of a cyberattack.

Traditionally, three interrelated components, the 'three Cs', are considered the necessary elements of successful deterrence: capability, credibility, and communication. A defender needs to have the necessary capabilities to inflict harm upon an attacker after being attacked (punishment), as well as the capabilities to defend against an attack or to deny either the weapons technology or the success of an attack (denial). Second, the challenger needs to believe that the defender is willing

and able to execute a retaliatory strike or is indeed able to defend or deny. Third, the defender should communicate to the challenger what to expect if he chooses to attack so that risk calculations can be made.

The capability to attack in cyberdeterrence consists of the knowledge of the vulnerabilities in an opponent's systems and the ability to exploit them. In this domain, in which 'weapons' are quasi-invisible, capability can be demonstrated indirectly, e.g., through institutionalization of cyberwar capacities in the form of cybercommands or directly by allowing attribution of sophisticated cyberattacks. For many observers, Stuxnet, the worm that sabotaged the Iranian atomic program, is such a case: Even though the US government has never officially confirmed its involvement, its key role is considered a fact in the international community and thereby serves to demonstrate and communicate the US has the capability and willingness to use an advanced cyberweapon against an adversary.

The credibility of one's ability to punish an attacker is linked to the possibility of attribution. True technical attribution in cyberspace is often impossible, especially in the case of APTs. However, the interesting trend that has become discernible is that there are in fact many cases of attribution in cases of cyberaggression, the latest being the identification of North Korea as the main perpetrator behind the Sony Hacks of 2014 by the US government. There are several aspects of importance: One, the norm is to apply the *cui bono* logic – to whose benefit – as the next best thing to true attribution, justified by the fact that cyberaggression hardly ever takes place in a strategic vacuum. Two, attribution is linked to the ability to fuse many sources of intelligence, some of which might be linked to APTs that are inside a potential enemy's networks already. Three, credibility is linked to the emerging norms in cyberconflict. By establishing clarity regarding what can be considered an armed attack in cyberspace and when escalation to another domain (i.e., conventional countermeasures) is possible, the costs of an attack become clear, and a more credible threat to escalate can be made.

The capability to defend or deny in cyberdeterrence, on the other hand, is linked to active and passive defensive IT-security measures and the resilience of systems. Resilience signifies the ability of systems, by means oftechnical, social, and political aspects, to deal with interruptions or crisis without breaking down. There are additional elements at play here,

such as being able to identify and to patch the biggest vulnerabilities in critical infrastructures. Establishing credibility in this domain is very difficult, considering the near-constant reporting of breaches in all kinds of networks. However, cybersecurity, cyberdefense, and resilience strategies can serve as declaratory elements to communicate institutional capabilities, for both, punishment and denial, and intentions. The case of five Chinese military officers indicted by a US court can be seen as such a declaratory action too: It signals that state actors are not immune from the law and establishes fairly clear red lines against cyberespionage for economic advantage.

The side-effects of normalization

Given the resources that states have at their disposal, they have been singled out as most dangerous threat actors in this security domain. On the one hand, the trend of stabilizing political interactions in and through cyberspace thus has positive effects by reducing the risk of escalation. Still, the stabilization of cyber-international relations has been a slow process, and many observers are highly critical of the actual effects, given how easily rules can be altered and agreements broken.

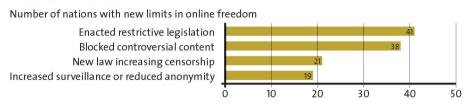Overall, it is too early to make conclusive statements about how effective the slowly emerging cybersecurity governance complex will be in the future in enhancing security. However, two related side-effects are already clearly discernible: The first is related to the focus of states on states as most dangerous actors, which causes more resources to be spent on pacifying state-to-state relations and fewer efforts to be expended counteracting malicious non-state actors and creating greater cybersecurity together with private actors. The second side-effect concerns the focus of the emerging cybersecurity governance complex on cyberattacks.
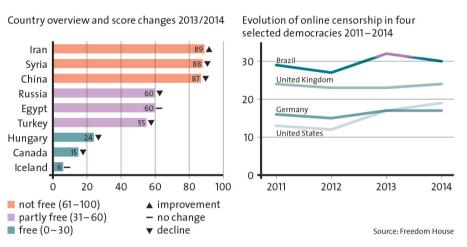
States, power, and cyberspace

As states are showing their willingness to place security needs above any other need when looking at cyberrelations, a widespread 'cyberutopia', which has dominated large parts of the information age, is coming to an end. For years, pundits have assured themselves of the powerlessness of states in the virtual realm and have shaken their heads at the attempts to respond with traditional tools to various policy issues concerning cyberspace. However, they had to realize that cyberspace may be different, but that the rules of the game can still be changed – by states. Concepts, such as 'Cyber-Westphalia', which lauds the benefits of order in the virtual space, based on the norms of

Freedom on the net 2014

Number of nations with new limits in online freedom

Enacted restrictive legislation	41
Blocked controversial content	38
New law increasing censorship	21
Increased surveillance or reduced anonymity	19

Country overview and score changes 2013/2014

Country	Score	Change
Iran	89	▲
Syria	88	▼
China	87	▼
Russia	60	▼
Egypt	60	–
Turkey	55	▼
Hungary	24	▼
Canada	15	▼
Iceland	6	–

■ not free (61–100)   ▲ improvement
■ partly free (31–60)   – no change
■ free (0–30)   ▼ decline

Evolution of online censorship in four selected democracies 2011–2014

Brazil
United Kingdom
Germany
United States

Source: Freedom House

sovereignty and power concentration in the hands of states, have guided the actions of the international community in the last few years. While international talks have increased in intensity and numbers, this has also meant more control of 'national' cyberspace – which always equals more control over information flows. Authoritarian governments are embracing this growing 'cybersovereignty' movement to further consolidate their power. In democratic states, there is more government surveillance and more censorship than ever before.

But while there are many positive signs of more stability and normalization in the international realm because of this recent focus on state-to-state relations, this seizing of power by states is not uncontested. Because cyberspace is a realm used by different actors for highly diverse activities, the security-seeking actions by states often directly clash with other uses and conceptions of cyberspace. This causes considerable resistance to the actions of governments, with high costs for all sides. In particular, there are problems associated with

the empowerment of intelligence and military establishments in matters of cybersecurity. The military accumulation of cybercapabilities may be outpacing civilian comprehension and control. Similar problems hold true for intelligence agencies: While they may have the budget and technological resources that are best suited to respond to cyberthreats, their role also elicits great public unease. Public disquiet over government surveillance and cyber capabilities could prove to be difficult for cybersecurity strategies in the future.

Cyberexploitation as destabilizer

The second side effect is the result of the very specific focus of cybersecurity norm-building on destructive cyberattacks. Normalization and stabilization efforts are geared towards a form of cyberaggression that could indeed be devastating, but that also has a low probability of occurrence. The biggest current issue, besides cybercrime, is cyberexploitation, which is done with the help of APTs: the world of intelligence communities, whose actions in home states are regulated by national law, but who are expected to act unfettered and without restraint in the international realm.

In that sense, the perennially insecure cyberspace is an Eldorado for actors who are interested in collecting data.

The big problem in cyber-international relations is that continued cyberexploitation by certain state actor threatens to undermine any stability that can be created through norms. They are making cyberspace more insecure directly, in order to be able to have more access to data and in order to prepare for future conflict. Edward Snowden's revelations in 2013 exposed that the NSA had bought and exploited vulnerabilities in current operating systems and hardware to inject malware into numerous strategically opportune points of the internet infrastructure. It is unknown, which computer systems have been compromised – but it is known that these backdoors or sleeper programs can be used for different purposes, as forsurveillance, espionage, and disruption, for example, and activated at any time. It has also been revealed that the US government spends large sums of money to crack existing encryption standards in the name of counterterrorism – and apparently has also actively exploited and contributed to vulnerabilities in widespread encryption systems.

The crux of the matter is that backdoors and unpatched vulnerabilities reduce the security of the entire system – for everyone. Strategic exploitation of vulnerabilities in computer systems and the weakening of

encryption standards have the potential to destroy trust and confidence in cyberspace overall, which would be a disaster from an economic perspective. Neither is there any guarantee that an intelligence actor who has acquired knowledge about an exploitable vulnerability, has full control over it and/or can keep it secret. Capabilities in cyberspace are a derivative of knowledge. Hence, they can just as well be identified and exploited by criminal hackers or even 'terrorists'. The OpenSSL Heartbleed bug that was exposed in 2014 is a case in point: there is evidence that the NSA knew about this flaw and kept it secret, in order to be able to exploit it for intelligence purposes. Leaving crucial vulnerabilities open deliberately will also nullify attempts to make deterrence logic work in cyberspace: If deterrence by punishment is not credibly linked to deterrence by denial, which ultimately requires a very active anti-vulnerability policy, it will not be able to unfold any effect.

Conclusion

States are back in cyberspace – and they are rapidly expanding their power in an attempt to gain more security. The trend is to invest in state-to-state relations to normalize cyber-international relations, focusing mainly on transparency measures and attempts to create deterrence effects through norm-building. This is currently giving rise to hope for more stability, as the risk of escalation is reduced. Overall, then, a secure, safe, and open cyberspace is not possible without involvement and commitments of states. At the same time, states remain the biggest threats to stability. State practices linked to cyberexploitation are emerging as a major part of the problem, constantly creating more insecurity and, in fact, also hindering the removal of known insecurities.

It is clear from recent developments that we cannot have both, a strategically exploitable cyberspace full of vulnerabilities and a secure and resilient cyberspace. How, then, can this problem be overcome? Because cyberspace is shaped and used by many non-state actors, solutions are not to be found solely in the cooperation between states. Rather, a focus on a common issue of interest for all stakeholders interested in more security is needed. Computer vulnerabilities constitute such common ground. In other words, if the goal is a secure and resilient cyberspace, then then active efforts are required to reduce strategically exploitable vulnerabilities in cyberspace This is a compromise that some state actors need to make if they want the type of national security that extends to cyberspace. If such a compromise is not achieved,

the dilemma will remain: The quest for more national security will always mean less cybersecurity, which will always mean less national security because of vulnerabilities in critical infrastructures. ●

CSS
ETH Zurich

STRATEGIC TRENDS offers an annual analysis of major developments in world affairs, with a primary focus on international security. Providing interpretations of key trends rather than a comprehensive survey of events, this publication will appeal to analysts, policy-makers, academics, the media and the interested public alike. It is produced by the Center for Security Studies (CSS) at ETH Zurich. Strategic Trends is available both as an e-publication and as a paperback.

STRATEGIC TRENDS 2015 is the sixth issue in the series. It features chapters on the Russian challenge to the liberal model of Europe, the danger of a Thirty Years' War in the Middle East, the effects of the rise of the so-called 'Islamic State' on international terrorism, current dynamics with regard to the militarization of space, and, finally, the gradual normalization of international relations in cyberspace.

The Center for Security Studies (www.css.ethz.ch) at ETH Zurich specializes in research, teaching, and the provision of electronic services in international and Swiss security policy. An academic institute with a major think-tank capacity, it has a wide network of partners.