Canadian
Security
Intelligence
Service

Service
canadien du
renseignement
de sécurité

2018 Security Outlook

Potential Risks and Threats

A FORESIGHT PROJECT

Canada

Occasional Papers 2016-06-03

This report is based on the views expressed during, and short papers contributed by speakers as part of, a series of presentations organised by the Canadian Security Intelligence Service under its academic outreach program. Offered as a means to support ongoing discussion, the report does not constitute an analytical document, nor does it represent any formal position of the organisations involved. The presentations and papers were offered under the Chatham House rule; therefore no attributions are made and the identity of speakers is not disclosed.

www.csis-scrs.gc.ca

Published June 2016
Printed in Canada

2018 Security Outlook

Potentials Risks and Threats

A foresight project

Table of contents

The project and its objectives

Academic Outreach at CSIS

Canada’s human intelligence agency, the Canadian Security Intelligence Service (CSIS) established an Academic Outreach program in 2008. The program seeks to help our own experts benefit from a dialogue with non-governmental specialists, foster our contextual understanding of evolving security issues and play a catalytic role in the world of research. Several of our activities—seminars, conferences, workshops—lead to the production of reports, which we now make accessible via our web site. Although the majority of our efforts aim to improve our understanding of issues of immediate priority to the Government of Canada, we also lead initiatives to explore emerging security developments that may have repercussions for Canada further into the future. Together, those initiatives have helped us adopt our own approach to the practice of foresight.

A look at 2018

The Academic Outreach program ran a multi-part foresight initiative from September 2015 to May 2016. Five leading global thinkers were commissioned to explore the drivers influencing the security risks and potential threats related to specific regions of the world and themes by the year 2018. This end point may seem arbitrary, but was deliberately selected to maximise the relevance of the foresight project in its aggregate. It is neither too far into the future so as to become overly abstract, and yet it is sufficiently remote from the present to allow contributor and reader to question current assumptions.

The result is this report. Through the examination of a broad range of challenges linked to China, the Middle East, Russia, weapons of mass destruction and cyber-security, it provides a glimpse into the dynamics that may be influencing the globe’s near-future. It may be that some of our interlocutors hold ideas or promote findings that conflict with the views and analysis of the Service, but it is for this specific reason that there is value to engage in this kind of conversation.

Executive summary

Executive summary

Overview

Over the next two years, there is a high potential for dangerous global instability.

- Both China and Russia have leaders with aggressive foreign policy agendas capable of generating diplomatic and military confrontations. However, while pursuing their objectives, both leaders must cope with structurally weak economies.

- Conflicts in Iraq, Syria, Libya and Yemen will continue. Multiple militia groups complicate attempts to end the violence in these countries, while affiliates of the Islamic State in Iraq and the Levant (ISIL) and Al-Qaeda spread insurgency and terror attacks across the Middle East, Africa, Asia and cities in Europe. There are few agreed principles on which to build comprehensive peace agreements, but negotiations may lessen the intensity of some conflicts. Neither Al-Qaeda nor ISIL affiliates are part of negotiations.

- The development and use of weapons of mass destruction (WMDs) will be a continuing focus of concern. While weapons technology will not leap ahead as fast as information technology, the risks of proliferation, or miscalculation, will continue to require constant monitoring and attention.

- North Korea as a developer of nuclear weapons and ballistic missiles remains a country of high concern. India and Pakistan, both nuclear powers, continue to have a confrontational relationship. Some non-state actors have already acquired the capabilities to produce and use chemical weapons. Despite the challenge, they will also likely attempt to use "dirty bombs".

- The potential for the Internet and cyber technology to be a strategically disruptive force is high, even within the next two years. Rapidly evolving information technology and cyber threats will continue to be a major preoccupation for states, non-state actors, private companies and ordinary citizens.

- US foreign policy continues to have much influence on the behaviour of countries in the Middle East and Asia. US global engagement is important to countries considering the acquisition or possible use of weapons of mass destruction. Therefore, the foreign policy of the person elected in November 2016 as President of the United States will be a major determinant of international dynamics over the next two years. Leaders of the US, Russia and China will interact on crises in the Middle East, the South China Sea and the periphery of Russia.

China at a crossroads

President Xi Jinping has reversed elements of China's collective leadership and asserted greater personal authority. This has had implications for both economic policy and domestic and foreign security strategies.

- Xi has asserted the importance of one supreme, visionary leader. He is now committed to creating a personal leadership cult which cannot be easily reversed. He is not politically vulnerable in the short term, but the longer term is uncertain. Both the new regime style and the man are brittle.

- The transition to an economy led by domestic consumer demand is not going smoothly as Xi tries to combine a market economy with central economic direction. Fear of the consequences of arbitrary measures is leading to an outflow of capital. This hybrid of central direction and a market economy can survive in the next two years. In a complex domestic and international economy, however, it is not viable in the longer term.

- China's policy of confrontation in the South China Sea is tied to Chinese national pride. The reaction of US regional allies depends on their degree of confidence that the US will fulfill its commitments. The linkages between Chinese policies, regional reactions and US intentions, increase the potential for conflict, possibly stimulated by an International Tribunal ruling on the South China Sea dispute. China also faces the alienation of Taiwan from China's increasingly authoritarian regime, and worsened relations with either the US or North Korea over the latter's nuclear and ballistic missile program.

The Middle East's political fabric

Instability in the Middle East has been driven by the unresolved question of the role of religion in public life. The Muslim Brotherhood model of democratic competition has been replaced by ISIL's belief in extreme violence to establish and govern a so-called caliphate.

- The coup in Egypt which removed the Muslim Brotherhood from power, as well as the Rabaa massacre of Brotherhood supporters in August 2013, have discredited the Muslim Brotherhood's advocacy of democratic engagement. A lesson from the Egyptian experience appears to be that the demands of Islamist state-building and the requirements of democratic power-sharing cannot be reconciled.

- In Egypt and some other Muslim-majority countries, Islam has historically been a force for national unity. This can change when an explicitly Islamic agenda is embedded within a political party's program. There is then a risk that a political-religious competition for power will generate a cycle of distrust, repression and destabilisation.

- ISIL has taken territory, declared the establishment of a caliphate, and instituted its own governance structures. The notion of the caliphate is very popular for many within the Muslim world. Whatever its eventual fate, the ISIL caliphate will serve as a model for future extremist militias which believe they can take control of territory and establish a governance structure.

Predictable Russian unpredictability

Russia is handicapped by poor economic performance but there is no evidence that this is hindering the consolidation of President Vladimir Putin’s absolute authority or the program to modernise Russia’s military.

- Western assessments that Russia is vulnerable to economic collapse and disruptive internal discontent are exaggerated. Russia is adapting to adversity; the economy is deliberately tilted to security rather than economic freedom. Political power in Russia is being steadily concentrated at the national level in an attempt to overcome system dysfunction in delivery. The current regime appears to be coherent, durable and united at the centre.

- Russia sees itself as surrounded by an arc of instability and chaos, and engaged in a “clash of civilisations”. It attributes conflict on its periphery to Western malice and incompetence.

- Two trends should be emphasized. First, Russia is not modernising its military primarily to extend its capacity to pursue hybrid warfare. It is modernising conventional military capability on a large scale; the state is mobilising for war. Second, on the important issues which generate international tensions, the regime does not change its policies: it reinforces them.

Weapons of Mass Destruction

The risk of the use of WMDs, or of a significant increase in proliferation, is low over the coming two years. However, technologies and expertise will continue to proliferate. This will increase the long-term danger that nuclear and chemical weapons, as well as ballistic delivery systems, will reach more countries, with a corresponding greater risk of use.

- International trade, the movement of populations and instability in some countries enable the spread of WMD expertise. There appears to be little prospect of a corresponding improvement in proliferation control-related mechanisms. The urge to acquire WMDs will continue to depend on: regional power balances; military intervention, particularly from Western powers; and whether regimes are liberal democracies or authoritarian. Perceptions of the new US President will be an important factor.

- Saudi Arabia, China, North Korea, Iran, Pakistan and Russia are the high-risk countries for acquisition, transfer or use of WMDs, while Russia and North Korea are potential exporters of ballistic missiles. North Korea remains the most unpredictable country with a potential nuclear-weapons capability. Tension between India and Pakistan represents the greatest danger of a direct confrontation between nuclear-armed states.

- Iran's behaviour over the next few years will signal its attitude to the agreement on terminating nuclear weapons development, and on its future intentions when the agreement expires.

- Some non-state actors may use drones to deploy their WMDs. ISIL already has chemical capabilities. It and others may be tempted in the coming years to enter the biological and radiological realm.

Cyber Threats

Cyber-insecurity will remain a major threat to states, private sector companies and individuals. The high rate of technological innovation, the dominance of commercial, off-the-shelf software, and the increasing proliferation of entities with embedded and unchangeable software means that cyber-attack potential will stay ahead of defence capabilities.

- The continued use of commercial technology means that system vulnerabilities can be known, traded and widely exploited. Interdependence based on linked networks makes important systems highly vulnerable to rapid and catastrophic collapse, requiring a prolonged repair stage. As the number of cyber transactions increases, the relative proportion of attacks may go down. However, the risk of catastrophic attacks is steadily increasing.

- The proliferation of devices with embedded systems—the Internet of Things—adds a new danger. Devices will be long-lasting, vulnerable to attack, but unreachable for software fixes.

- The state use of cyber-attack weapons will not be restrained as the use of nuclear weapons was because cyber-attacks are difficult to trace to the attacker.

Considered from the perspective of the topics covered in this review, the period 2016 to 2018 must be assessed as one with significant risks of destabilising developments and increased international tension.

CHAPTER 1

China’s dangerous years ahead

Chapter 1 – China's dangerous years ahead

Predicting the future of China is a risky undertaking. The accepted wisdom is that Chinese history moves in cycles, involving long periods of stability followed by the loss of legitimacy and either chaos or revolutionary change. As in any authoritarian system that produces brittle politics and institutions, it is hard to second guess the timing of those changes. Even if one believes that something in the system, or even the whole system, must snap at some point, it remains possible that authoritarian mobilisation can delay the breaking point to a later date. To the leaders of such systems, it is in fact the whims of democracy that bring the risk of sudden and unwarranted change.

During the Deng Xiaoping era, adaptation and reform, either in bursts under his stewardship or incrementally with his successors, took care of the issue. Deng in fact communicated a sense of time—for example, a 50-year deal for Hong Kong or postponing the resolution of China-Japan territorial issues "to the next generation". The two most influential reports on reforms under the Hu-Wen leadership were both entitled "China in 2030". Xi Jinping, however, has not formulated such a time horizon as he tightens his personal grip over the country. Authoritarian regimes have no deadline; they do not entertain an expiration date, whereas democracies live through election cycles. Instead, analysts of China are often influenced by a combination of policy and dynastic cycles: the former well exemplified under Mao, and again with the vagaries of reform after 1979; the latter always uppermost in the leaders' minds, making the continuation of the regime the number one priority at any cost.

An upheaval from below, following a visible loss of regime legitimacy, is always possible. Yet the tools of political control acquired by a coercive and resource-rich regime, combining mass campaigns and technology, are formidable. Shaking the system from above has been absolutely excluded, following Mao's initiatives that were disastrous to his colleagues, as well as to the general population. Under Deng Xiaoping's leadership, the fate of his two successive lieutenants, Hu Yaobang and Zhao Ziyang, who tried to rock the boat in 1986 and 1989, illustrates that prohibition. Xi Jinping has pointed to former USSR leader Mikhail Gorbachev as the model of what must not happen to China and the Chinese Communist Party (CCP).

The first three years of what can now be called Xi Jinping's reign have amplified these rigidities. Any move to the rule of law has been excluded (as opposed to rule by law under the Party and state bureaucracy), whereas there had remained previously some ambiguity. Repression of activists of any kind, and of their legal defenders, has intensified to a degree unknown since Mao's death. Even collective leadership has been reversed, with Xi's colleagues presumably cowed by the anti-corruption campaign, and Xi Jinping increasingly designated as the "core leader". The long arm of Chinese state security is spreading abroad, in Hong Kong, Thailand, Australia and even the United States. Reform, only three years ago (2011-2012) hinting at a major top-down development, is now bottoming out as a myriad of small administrative and technical changes, with no visible flag bearer. Communist ideology, the achievements of the 1950s and Mao as a primeval figure have been revived with an increasing role for the Party's propaganda department. If Xi Jinping denounced Gorbachev as a liquidator, he is positioning himself as a restorationist of the CCP, to use a term that is both Leninist and Qing dynasty parlance.

Major trends impacting the Chinese political scene that could puncture the armour recreated by Xi Jinping

A reversal of fortune for China's economy

This author belongs to the school that believes international commentary, after hyping China's miraculous growth, is exaggerating today the degree of economic emergency the country is supposedly facing. Not only was slower growth predicted, it was actually willed by at least some reform-minded leaders in the previous government team. But the framework for transition (from resource- and investment-intensive growth to a consumer, service and high-tech economy) is now being derailed. There has been a highly visible mishandling of stock market regulatory issues and monetary liberalisation. A continuing hesitation about the risks from slower growth led in 2015 to another wave of credit-based stimuli to the economy. But this came without the growth that it previously sustained: in other words, China is getting both runaway public stimuli and lower growth.

These are now impacting the aura of management invincibility that has protected the Chinese leadership. At best, this is a communication disaster. At worst, it reflects a misunderstanding of economic rules at the top: the leadership believes it can run side by side elements of an internationally attractive market system and heavy-handed correction of these same markets. In turn, this has created a second event: China's firms with international connections, and China's individual citizens with assets to protect, are both running abroad for cover. How else to interpret the outflow of capital—USD 1,1 trillion in a year[1], now running at more than USD 100 billion per month? Explanations, such as firms and individuals winding down their dollar bets and anticipating dollar purchases, or the decline of other currencies held in China's reserves, or even fabricated export data, are a description of how the outflow happens rather than a counterfactual.

There is no rational explanation for this, but two psychological factors. One is the belief that the dollar will keep rising and that the yuan will leave its peg and devaluate, whether that is a goal for the leadership or not. The second factor is the growing fear of arbitrary moves threatening acquired wealth and business. Corruption was always seen as a cost of doing business and as a road to fortune for China's upper middle class and entrepreneurs, who are usually well connected. It is the people below who resent it. The campaign led by Xi Jinping and CCP inspection chief Wang Qishan has triggered a Latin American-type capital exodus by the rich.

A major international test over China's assertiveness in the East and South China Sea

On the surface, the terms of the issue are reassuring. Except with Vietnam (1974, 1988 and 2014), a nation bereft of allies, China has certainly tested several red lines but never crossed them. For their part, neighbourhood economies are so interlocked with China that they act as a restraint—even for Japan, the country with the biggest incentive to call what is still China's bluff rather than face later a military superpower. Meanwhile the United States has made the unspoken concession of 'grey areas' where Chinese assertive behaviour is tolerated without triggering alliance counter-actions. There are currently three such grey areas. One concerns intrusion in waters under Japan's administrative control around the Senkaku-Diaoyu islands—with fishing boats, then with China's naval agencies' lightly armed boats, and for the first time by an armed frigate in December 2015. Another is the stand-off around the Philippine's Scarborough Shoal since June 2012: after retreating from outright military conflict, China has blocked all

Filipino access to the area, and the United States has not backed its assurances made in early 2013 to ensure free access by others to their island features. A third grey area is freedom of navigation, whether at sea or in the skies. Although the United States challenges China’s restrictions, China’s actions remain a deterrent to others, who confine their protests to words.

This situation is full of immediate dangers. First, the applicability of US commitments is at least doubted by its regional allies, and most of all by Japan. They may be tempted to test those commitments. Second, even though the Xi regime is regaining control of China’s public opinion and its nationalist outpourings, it remains vulnerable to a set-back in the area of sovereignty and national pride. It may in fact be the fear of a larger backlash from Chinese public opinion that has prevented Japan from devising a local pushback. Three, the potential for accidental conflict is growing. China’s recent installation of surface-to-air missiles in the Paracels broadens these possibilities.

After the terrorist attacks of 11 September 2001, US strategy in the Asia-Pacific refocused on stability over change. The concession was broadly successful until late 2009. It is now being challenged by China, and remaining areas of cooperation—North Korea, climate politics, the IMF, accommodation at the UN—are wearing very thin. Xi Jinping also appears to have a credibility issue—his September 2015 declaration, while in the United States, that "China does not intend to pursue militarisation" in the South China Sea ranks on a par with some of Vladimir Putin’s statements over the Ukraine crisis.

A political challenge from within the regime

Xi Jinping seems to believe that tightening all screws—from media and propaganda to surveillance, the judicial system and Party control over all administrations—as well as taking almost all matters under his personal authority is the only way to avoid the weakening of the regime and ultimately the downfall of the CCP. His closest aide, Wang Qishan, who heads the feared Party Central Commission for Discipline Inspection, had repeatedly advised cadres in 2012-2013 to read Alexis de Tocqueville. Most relevant to China is of course Tocqueville’s observation that regimes are most at risk when they initiate reform. The Xi-Wang team’s governance mix consists of a struggle against political corruption that doubles as a tool for control, minute prescriptions to change rules that are often not fully implemented, and a radical refusal of any political reform.

The mix is dangerous. In one top-level Chinese expert's views, Xi Jinping attempts to be "both Mao and Zhou", that is the unpredictable Great Helmsman and the meticulous administrator rolled into one. Prime Minister Li Keqiang has so disappeared from view that even gossip about him is now very scarce, as if his presence does not really matter. Li's foreign travel schedule is also scant, whereas Xi Jinping himself is very often abroad.

Xi's regressive politics are a throwback to the Mao era but not a return to Mao. Mao is an overarching figure and a deterrent for those tempted by political change, but he is not to be idolised again—instead, elements of a Xi cult are setting in. This can only be intentional. In fact, the highly unusual interview he gave to a Chinese magazine in 2000, titled "How I entered politics[2]", seems like a take on Edgar Snow's famous interview of Mao in 1936[3]. What seems clear is that Xi cannot afford to walk back from the restoration of personal rule that he has implemented. Lifting the fear that now hangs over his colleagues and all activists would result in a powerful backlash from any of these quarters, as his moderation would be interpreted as weakeness. A real question is his future psychological balance. The man has appeared ductile, adaptable and well able to manage contradictions, including in his close family (with a beloved daughter long at Harvard University, a complete oddity given his prescriptions). But sycophancy, underestimation of economic realities, and the issue of personal face are elements that caused Mao Zedong's and the country's tragedy. Interestingly, Xi Jinping has never recognised publicly having made a single mistake.

The psychological risk from absolute power is very real. Xi has ended the unspoken truce that forbade Party leaders from seeking the physical elimination or jailing of their peers. A visible failure in China's foreign policy or in economic policy would result in a challenge to his power from within the regime—or an even more pronounced turn to autocratic methods. Only two years ago, the money was on a shift by Xi Jinping to 'consultative Leninism', combining input from experts and from below with the possibility of decision or arbitration from the top. That line of thinking is over.

What are the possible scenarios for the next two years?

From the bearish outlook above, but with the reservation that it is not clear at what speed trends might set in, the following scenarios are possible.

Economy on the skids and the consequences

Even this dark scenario does not involve an outright crash, whether for the currency or the economy. The authorities have several fire breakers at their disposal: spending down currency reserves which would result in even greater trade competitiveness, rescinding some capital liberalisation measures inside or outside China, whether openly or through administrative 'guidance'. The greater risk today does not lie with the external account—strong capital flight is balanced by the trade surplus—but rather with the pile-up of domestic debt. The government has a choice between an economic crunch allowing for continued economic liberalisation, with a strong social and possibly political fallout. Or it can opt for further monetary loosening, which will transfer abroad part of the burden for adjustment, and force the re-imposition of more formal or informal capital controls. The dollar's rise offers opportunities for political cover. Other currencies, such as the yen and the euro, are much more vulnerable to a weaker yuan in terms of trade competitiveness.

Our scenario for the next two years has two parts. First, an anticipation of devaluation with capital flight—including high-profile acquisitions abroad by major firms and accelerated real estate purchases by China's wealthy class. In a second stage, the regime reacts by re-imposing more brakes and delinking China from global capital markets. This means fewer acquisitions abroad, diminishing or cancelling the existing bridges—such as the offshore yuan market, the Shanghai-HK connect, or the swap agreements with central banks.

In turn, this second stage lessens any incentive for China to cooperate internationally. It would face increased opposition to its mercantilism and dumping practices, since the countervailing factor of capital investment would be less important.

Politically, the implications are obvious. There could be a risk with China's IMF reserve currency status, which will be formally confirmed only in October 2016. In the meantime, the domestic balance between state-owned enterprises (SOEs) or protected sectors, on the one hand, and private entrepreneurship or the new economy on the other has become more important than external liberalisation debates. China's economy, once on a different course from that of an increasingly isolated political regime, is being realigned with the political system.

The longer term prognosis from this scenario is not good. It leaves no argument for political liberalisation, and external sources of growth are stifled, replaced by increased reliance on internal market forces and public push. Still, in the short term it is viable, even more so if the global economy tanks and other major economies also indulge in monetary competition or mercantilism. Also in the short term, the Chinese economy is no less competitive. On the contrary, its ballooning trade surplus is a constraint on global growth and could become a major liability outside China.

> *China's economy, once on a different course from that of an increasingly isolated political regime, is being realigned with the political system.*

Xi's mix of Party-driven policy at the core and laissez-faire economics at the margins could work in the low-income economy of ten years ago. Today's interlinked economy and finance, with its emphasis on technology and its increased channels to the outside world, require clearer choices. Unfortunately, they are politically contradictory with the way Xi Jinping has developed his mandate: he can only threaten members of his ruling class because he guarantees their collective survival.

Calling China's bluff on the sea

Given Xi's preference for hard management of all issues involving public opinion and the media and his absolute rejection of democracy, it is not surprising that the growing political hostility to China among neighbouring Asian countries leaves him indifferent. Rather, he must tabulate the victories on the ground scored by China over recent years.

The problem is that China may be running out of easy victories. Relations with Taiwan may be taken as an example. China has drawn Taiwan much nearer. But even outgoing Taiwanese president Ma Ying-jeou, who clings to the 1992 Singapore consensus formula of “one China, respective interpretations[4]" in order to constrain independentist temptations after him, did not move forward on political relations with the People’s Republic of China (PRC) during his terms in office. The East China Sea Air Defence Identification Zone (ADIZ) may have already been a bridge too far, although not insisting on its thorough implementation represents a temporary phase. China has in practice gained access to the Senkaku-Diaoyu’s territorial waters, while Japanese fishermen are now constrained by their own authorities from entering these waters. With a quasi-military ship, China is skirting the red line again—going one step further carries enormous risks. In the South China Sea, Beijing is on the way to achieve the means of surveillance and some aerial interdiction capacity. This will make it harder to stick to vocal protests when the United States enforces the doctrine of free navigation. Yet a practical clash would have enormous repercussions. Meanwhile, nearly every Asian neighbour is rearming.

A first test could come by mid-2016. If and when the International Tribunal rules in favour of the Philippines, it is nearly certain that China will contest the validity of the ruling and abstain from implementing it. What next? The Philippines, eventually encouraged by a discreet group of Asian partners who want to recommit the United States to its alliances in the region, could mount a practical challenge that would seem peaceful: navigation and resupply of islets currently fenced in by China’s Oceanic Administration or Coast Guard ships. This challenge is more likely to happen than the widely predicted conflict between China and Vietnam. Although Vietnam has made a strong public diplomacy offensive, it has refrained from going to court, effectively vying for a separate settlement. Unlike Crimea or Donbass, this scenario involved no runaway activist groups, and can therefore be strategised as a way to call China’s bluff. With the US presidential campaign in full swing, reactions from the Washington are harder to anticipate.

A second test is obviously over the Taiwan issue. At a time when China has chosen to rein in public opinion in Hong Kong, it will be difficult to let new President Tsai Ing-wen display marks of national pride, if not independentism, over Taiwan. In both cases—Hong Kong and Taiwan—public perceptions of China’s return to greater authoritarianism have shifted opinion against the PRC to levels unseen since 1989.

A third test may come over North Korea. It may be tempting to see recent North Korean actions—a fourth nuclear test and a ballistic missile-cum-satellite launch, as merely the continuation of an existing trend. Yet the credibility of the United States is at stake, and that of China's strategic cooperation too: North Korea is, with climate issues and China's status at the IMF, the only three real areas of cooperation between Beijing and Washington. Climate cooperation has been overturned within the United States (with a negative Supreme Court ruling) and cooperation over monetary issues is likely to sour with China's new economic circumstances. That leaves North Korea as the only positive, if China agrees to stronger sanctions. In short, within the next year, China has a choice between antagonising the United States on yet another issue, or facing down the North Korean leadership, with all the consequences it loathes: losing the card with the United States by playing it and destabilising the Korean peninsula. In exchange, however, China would momentarily gain unprecedented leverage with South Korea, but this cannot be guaranteed over time. In such a situation, our more likely scenario is a worsening of relations with the United States.

A power struggle at the top

This is a tempting hypothesis. Xi's return to personal power, his use of the anti-corruption weapon to political ends, his growing threat to the tranquility and prosperity of China's upper middle classes, as well as the social fall-out from a sectoral and geographically focused slowdown all point to potentially strong discontent. The exceptional degree of control over public expression and the media that he is achieving could act as a pressure-cooker. A challenger with a position of legitimacy might suddenly find much support.

It is not inconceivable that such a challenge would happen. Over the past few years, this is exactly what Bo Xilai and Zhou Yongkang attempted to do, partly in cooperation and partly in succession.

But this goes against the statistical record. No Number 2 (or 3, or 4…) in the CCP has ever unseated a Number 1 (except Mao in the revolutionary phase of the Party). The only revolts from below, beyond localised 'mass incidents', that have met with at least temporary success were encouraged from above by the Number 1. Factional politics rule the avenues for discontent, but as the new core leader, Xi has enough of a deterrent to challenges from colleagues. Opposition from the People's Liberation Army (PLA), often cited in the past few years, has been cowed through large personnel changes and the anti-corruption drive. The only surprise happened recently when General Liu Yuan, the son of former leader Liu Shaoqi, a stalwart nationalist and anti-corruption voice, closely acquainted with Xi, was retired instead of being promoted further. We hypothesise that Xi does not want a sole strongman in the PLA, not even a close relation. In fact, Xi's military purge is very similar to the one carried out by North Korea's Kim Jong-un, minus the physical violence, so far.

A loss of prestige or face resulting from a policy failure would probably result in a harder stance by the top leader. The 'president of everything' has taken on almost all factions whose mutual hostility allowed him to gain personal power. This leaves only room for the promotion of personal followers from his earlier career—in other words, cronies. Speculation that he will build up his own faction at the 19th Party Congress in 2017 neglects the fact that he leaves no other faction standing. The psychological risk from absolute power is very real.

What we face is a reign which has only started and has no predictable ending. An insightful Chinese expert noted privately that a key feature of Xi Jinping is his ability to change his policies: the example given was Japan, in which after having created a disaster he just turned around and gave up the issue. So with the 'Chinese Dream', and possibly with OBOR (One Belt One Road) now that exporting currency reserves is less of a necessity, and energy or raw materials become a buyer's market. Shouldering international responsibility, a key feature of Xi's speech at the 2015 United Nations General Assembly, faded away after a reportedly disappointing United States visit. For all their foibles, Jiang Zemin (in 2002 over the intervention against Saddam Hussein) and Hu Jintao (over the intervention in Libya in 2011) took on more responsible roles.

By contrast, personality cult has risen again, and could prove stronger than the restraints of the CCP Party Constitution or unspoken customary law. Few observers would venture that Xi is set to retire after ten years and two mandates in power. The same observers who want to predict a reformist Xi after the 2017 Party Congress also see him doing a ‘Putin act’ in 2022 by moving to direct elections with a constitutional rule. This is a pipe dream. Even Russia’s authoritarian regime by far has more restraints and democratic elements built into it than present-day China. Putin rides on public opinion, even if he engineers it. Xi does not need public opinion.

> *What we face is a reign which has only started and has no predictable ending.*

We are left with the long-term consequences of an authoritarian and brittle system, which has given up the areas of flexibility that Xi’s predecessors had kept alive. We do not see any short-term alternative scenario other than would come from an issue with Xi’s health. On the other hand, this does not portend stability as the man is fickle, opportunistic and occasionally violent.

CHAPTER 2

Drivers of Middle East conflict: The present and future of political Islam

Chapter 2 – Drivers of Middle East conflict: The present and future of political Islam

The breakdown of the Middle East did not begin in 2011. Ever since 1924, when the Ottoman caliphate was formally abolished, there has been a struggle to establish a legitimate political order in the Middle East. At the centre of that struggle is the unresolved question of the role of religion in public life and Islam's relationship to the state. If we begin with this framing, then the devastating events of the past several years (with each year seemingly worse than the one before) begin to make more sense. The current crisis is just the latest iteration of the "problem" of the modern Arab state, a problem which is only likely to intensify.

This is not the traditional Sykes-Picot argument—about the untenability of arbitrary and artificial states fashioned out of European colonial projects—that has become fashionable of late (although this artificiality is no doubt a problem). The arguments made here about the drivers of conflict have more to do with governance and legitimacy deficits that stem from the inability to replace pre-modern caliphal structures with something with as much, or more, legitimacy.

These drivers of conflict are not simply about politics and power in the normal sense. If so, they would be more easily resolved. The conflict is not primarily about economic divides (even if with an ideological cast), as it once was in Latin America. In countries like Chile in the 1980s, the socialist opposition could reassure neo-liberal elites that their material interests would be protected in any transitional process. It is one thing to split the middle on material interests—things that you quantify and measure—but how do you split the middle on religion, ideology and identity?

Egypt as a representative case

Egypt is what we might call a 'hard case' for the framework offered above. It is one of the least artificial Middle Eastern states. Egypt has had a relatively well formed sense of nationhood or 'Egyptian-ness'. A kind of Egyptian exceptionalism—captured in the popular phrase *umm al-dunya* ('mother of the world')—has long been part of the country's cultural and political discourse.

The idea of the Egyptian state, with its attendant bureaucratic largesse, predates Egyptian independence. For the near entirety of the post-independence era, the military, judiciary and the religious establishment may have been politicised, but they at least offered the pretense of being above the fray, nurturing an illusion of independence and autonomy. They were widely perceived, even by Islamists, as pillars of the state.

This ‘state-ness’, in addition to the fact that Egypt is one of the region’s more homogenous countries, would suggest, all other things being equal, a greater likelihood of economic and political success. This, though, has not necessarily been the case.

The politicisation of state institutions

Even for those who knew that the military had presided over any number of failures, both foreign and domestic, there was a sense that the military was out of bounds as a target of criticism. During the 2011 uprising, defying orders from President Hosni Mubarak’s associates, the army refused to shoot into the crowds, burnishing its image of non-partisanship. The army, ever conscious of its self-image, deliberately and consistently promoted the following message: they represented no party or faction; they were dutiful servants of the nation; and they would guard over the interests of Egypt and Egypt alone.

As recently as the mid-2000s, the judiciary was hailed for its relative independence and autonomy, often resisting the Mubarak regime’s authoritarian designs. Even under the rule of Gamal Abdel Nasser—considered, at least before Sissi, as representing the peak of Egyptian repression—the courts tried to maintain at least some distance from Nasser’s dismantling of the Muslim Brotherhood.

After the 2013 coup, state institutions readily gave up any pretense of neutrality. For the first time, the military—supported by all arms of the state, including the religious establishment—killed large numbers of Egyptian civilians from one particular political faction, in this case the Muslim Brotherhood and its allies. Once the Rabaa massacre of August 14, 2013 happened, it had become, in a sense, too late. Too much blood had been spilled.

The Muslim Brotherhood and the state

In the pre-2011 period, the Muslim Brotherhood, which had repeatedly fallen victim to the military’s manipulations throughout its history, avoided direct criticism of the army. To oppose the military would be tantamount to advocating revolution and Brotherhood leaders had little interest in dismantling or purging the state. If they needed to place blame, they could direct it at individuals or policies, but not at institutions. There was no need to alienate state institutions when they hoped, one day, to win them over through the democratic process. Why defeat the state when it could more easily be co-opted? This guided the group’s strategy during the Arab Spring. As one former Morsi administration official told the author, looking back at that critical period: “Our reformist approach led to a self-interested pact with the military[5]".

In the post-coup era, young Brotherhood activists inside Egypt—many of whom lambast the group’s conservative old-guard for not being “revolutionary” enough—increasingly see the state not as an adversary to be co-opted or reformed, but as an enemy to be undermined. The traditionally cautious Brotherhood leadership, feeling pressure from its younger rank-and-file, has adopted some of the same rhetoric. In this sense, the Brotherhood has most certainly learned lessons from the failed project of 2011-2013, even if they may not, in the view of outside observers, be the right ones. Various Brotherhood leaders have told the author that they do, in fact, have regrets; one of them is believing that the system could be improved gradually from inside.

When thinking about radicalisation, we tend to focus on the use of violence. But, intellectually and philosophically, attitudes towards the state and how to change it often prove more important over time. Violence is, more often than not, about means. The state is about ends.

The implications of this shift in Islamist perceptions of the Egyptian state are profound and are likely to haunt Egypt for a long time to come. Whether they are justified or not, revolutionary approaches to politics, particularly when they hit up against an intransigent state, are likely to create more instability, at least in the short term. Since the state has no interest in accommodating or incorporating them, both Islamists and secular revolutionaries have a greater incentive to play spoiler. In this sense, incentive structures are woefully misaligned in a way that encourages a spiral of destabilisation: opposition plays spoiler; the regime becomes even more repressive; revolutionary attitudes of opposition activists harden.

The state-centrism of mainstream Islamists

Mainstream Islamism—defined here as the political theory and practice of the Muslim Brotherhood and Brotherhood-inspired organisations—is often assumed to be in conflict with or even in direct opposition to the modern nation-state and the Westphalian order more generally[6]. This is not correct. If one had to sum up mainstream Islamism—the successor ideology to Mohammed Abdu and Jamal al-Din al-Afghani's late 19th century 'Islamic modernism'—in a sentence, one would describe it as the effort to reconcile pre-modern Islamic law with the modern nation-state. This is worth emphasising: Islamism is an inherently modern and modernist project and one that is, accordingly, state-centric. The scholar of Islamic law, Wael Hallaq, takes issue with Islamists for precisely this reason, arguing that they have become obsessed with the modern nation-state, to the extent of "taking [it] for granted and, in effect, as a timeless phenomenon[7]".

The project of political Islam, then, was—for better or, in Hallaq's view, worse—an attempt to resolve the ideological divide at the centre of the struggle for a post-caliphate order. Islamists did what they were supposed to do, particularly in the 1990s and 2000s as they came under greater pressure from Western interlocutors as well as secular parties at home to become more 'moderate[8]'. Yet the more Islamists came to terms with democracy, political parties, and the nation-state, the more they found themselves rejected and repressed.

Even in the best of circumstances (ie, Turkey), Islamist participation in the democratic process is inherently polarising, not just because of what Islamists themselves do, but just as much if not more so because of the responses from domestic and international opponents that Islamists inevitably provoke. Even when Islamists are not the problem, they *are* the problem. Even when they make historic compromises, as in Tunisia, they still provoke anti-democratic behaviour on the part of secular and liberal parties. (In Tunisia, leading secular parties called for the dissolution of either the democratically-elected constituent assembly or the government, or both).

In other words, polarisation is inevitable when Islam ceases to be, as it once was, a source of unity and solidarity and becomes instead the province of one political party. Islamism only made sense in opposition to something else, and that something else was secularism. Islam was no longer just a way of being. It was no longer the natural order of things (as it was in the pre-modern period), and so it had to be reaffirmed and reasserted. These Islamist parties then compete for state power, and when the state is strong and 'over-developed', as it has been in much of the modern Middle East, it raises the stakes considerably, adding to the existential tenor of political competition.

In short, state-centric solutions or solutions that privilege strong, centralised states may exacerbate some of the challenges discussed above. Another way of looking at it is that the demands of state-building—which require the accumulation and centralisation of authority—and the demands of democratisation—which require the balancing and distribution of power—can often be in conflict. Presumption that the former should always or necessarily take precedence over the latter should be questioned.

Transcending the state

If one had to pick a single headline from the Arab Spring, it would be the opposite of what one hoped it would be: violence actually works. This applies not just to extremist groups like the Islamic State in Iraq and the Levant (ISIL)[9] but also to authoritarian regimes that have been able to remain in power by doubling down on authoritarian measures and resorting to ever increasing levels of repression.

ISIL considers groups like the Brotherhood to be apostates, since they have reneged on the notion of God as the sole law-giver and insist on sharing his jurisdiction with that of elected parliaments. But its position is not just a theological one. ISIL makes very specific arguments about the failure of democratic processes. For example, in one recruitment video, a young Egyptian man—a judge in one of ISIL's Islamic courts—tells the camera that "[Islamist groups that participate in elections] do not possess the military power or the means to defend the gains they have achieved through elections.

After they win, they are put in prison, they are killed in the squares, as if they'd never even won (...) as if they had never campaigned for their candidates[10]".

This statement is not necessarily new. Al-Qaeda regularly made similar pronouncements during the mid-2000s, particularly after Iraq's Muslim Brotherhood took part in successive US-backed governments following the 2003 Iraq war.

Al-Qaeda and its ilk gleefully described the Muslim Brotherhood as *al-Ikhwan al-Muflisun*, or the "Bankrupt Brotherhood"—a play on its Arabic name. But while Al-Qaeda may have achieved a measure of sympathy in the Middle East after the attacks of 11 September 2001, it was never, and never could be, a real threat to the Brotherhood's model of political change. It was proficient at staging terrorist attacks, but proved unable to carry its successes into the realm of governance. More importantly, Al-Qaeda's vision for state-building, to the extent it had one, failed to capture the attention of the world or the imagination of tens of thousands of would-be fighters and fellow travellers. Moreover, during this period, Islamist movements, despite only limited political openings, were experiencing unprecedented success at the ballot box, in Egypt, Kuwait, Pakistan, Lebanon, Saudi Arabia and elsewhere, making Al-Qaeda's jeremiads against democracy seem out of touch with the times.

While secularists and liberals rejoiced over the 3 July 2013 military coup in Egypt, so too did radical Islamists like ISIL who saw this as a definitive vindication of what jihadists of various stripes had been saying for years. ISIL clearly thinks that it benefited from Morsi's overthrow. In ISIL's first statement after the coup, spokesman Abu Mohamed al-Adnani, addressing the Muslim Brotherhood and other mainstream Islamists, said: "You have been exposed in Egypt". He referred to democracy and the Brotherhood as "the two idols [which] have fallen[11]".

Unlike the Brotherhood, which believed in accepting the existing state and 'Islamising' it—just as they might 'Islamise' democracy, socialism or capitalism—ISIL believed in building on top of an entirely different foundation. This was a new and rather distinctive take on the applied Islam of modern-day Islamist ideologues. As we saw earlier, the tensions between the mundane requirements of governance and religious absolutism make for an uncomfortable mix. One would think that such tensions are magnified tenfold when it comes to a group like ISIL with unabashedly maximalist and even apocalyptic goals. Yet, in superseding the nation-state and the regional architecture—it has no state patrons—ISIL has managed also to supersede the endless contortions of mainstream Islamism. In other words, the totalising nature of ISIL is no mistake: it is inherent to the model.

There is little to suggest that this is sustainable in the long-run. As a seasoned observer of the Middle East has elegantly put it, "The caliphate may require caution but the apocalypse requires abandon". That this is ultimately unsustainable does not mean, however, that ISIL's model cannot inspire a small but vociferous minority throughout the Muslim world. It has and it will. More than that, even if it were defeated tomorrow, ISIL would stand as one of the most successful and distinctly 'Islamist' state-building projects of the modern era—of course, with the caveat that the bar is rather low. Still, this is no small feat and to the extent that one wishes to sensationalise ISIL, it should probably be on these comparatively mundane grounds.

> *…the totalising nature of ISIL is no mistake: it is inherent to the model.*

Even if it is often only implicit, ISIL is making an argument about how to establish 'proper' Islamic governance in the context of modern nation-states: to achieve fidelity to the text, one must start, basically, from scratch, since whenever Islamism and the modern state attempt to reconcile, it is always at the expense of the former.

This brings us to the sometimes circular and tiresome debate about whether ISIL is Islamic. A better question is: how does ISIL approach Islamic scripture? In the view of this author, it is difficult—impossible, really—to argue that Islamism has nothing to do with Islam, when it very clearly does, when one looks closely at the Islamists' approach to governance. As Yale University's Andrew March and Mara Revkin lay out in considerable detail, the group has, in fact, developed fairly elaborate institutional structures[12]. In the intellectual and theological realms, ISIL is not just Baathist brutality in Islamic garb; rather, it has articulated a policy towards Christian minorities based on a 7th century pact and attempted to develop a novel Islamic economic jurisprudence, as well as a heterodox theory of international relations. Of course, this does not mean that ISIL is anywhere near the mainstream of Islamic thought as practiced over the course of fourteen centuries—what is often referred to as the Islamic 'tradition'. In this sense, ISIL is on the far fringes of Quranic interpretation. This, though, is precisely the point. ISIL is not unaware of this; it basks in this. US expert Will McCants offers an interesting aside in this respect, arguing that "ISIL, in some ways, does horrible things to deliberately provoke a debate about the 'Islamicisity' [sic] of their actions, and they welcome the ensuing argument that breaks out[13]".

Part of the debate in assessing the Islamic dimension of ISIL has to do with problems of interpreting political and religious actors outside of their original context. For example, James Madison—one of the Founding Fathers of the United States and lead drafter of the Bill of Rights—would not be considered a liberal by today's standards, considering that he owned hundreds of slaves over the course of his life. Many of the philosophers of the Enlightenment in the 17th and 18th centuries opposed universal suffrage, believed in excluding certain groups (eg, atheists, observant Catholics) and generally feared mass participating in the political process. Yet, today, we celebrate them, because they were liberal in the context of their own time and place, not ours.

If ISIL existed twelve centuries ago, they would be controversial, and perhaps they would have been deemed heretics by some, but at least some of their acts—slavery, concubinage and waging war against established states for example—would not have been as jarring at a time when brutality in warfare was the norm; when the Westphalian order was still centuries away; when the notion of liberal democracy did not even exist; and when the idea of universal human rights simply would not have made much sense. In this respect, ISIL is distinctly modern. Few things, after all, are more modern than ISIL's ostentatious anti-modernism.

How much does religion matter?

In a September 2014 statement, ISIL spokesman Abu Mohamed al-Adnani expounded on the group's inherent advantage: "Being killed (…) is a victory", he said. "You fight a people who can never be defeated. They either gain victory or are killed[14]". In this most basic sense, religion matters, and it matters a great deal. As individuals, most (if not necessarily all) ISIL fighters are not only willing to die in a blaze of religious ecstasy; they welcome it. It does not particularly matter if this sounds absurd to us. It is what they believe. This basic point about intention and motivation does not just apply to extremist groups, but also to mainstream Islamist groups like the Muslim Brotherhood that work within the democratic process, contest elections and adopt a gradualist model of Islamising society. As one Brotherhood official told the author, many join the movement “so they can get into heaven”. Discussing his own reasons for joining the organisation, he explained: “I was far from religion and this was unsettling. Islamists resolved it for me[15]".

It would be a mistake, then, to view mainstream Islamist movements as traditional political parties. Muslim Brotherhood branches and affiliates are not just acting for this world, but also for the next. They aim to strengthen the religious character of individuals through a multi-tiered membership system and an extensive educational process with a structured curriculum. Each Brother is part of a ‘family’, usually consisting of five to ten members who meet on a weekly basis to read and discuss religious texts. For many members, it is quite simple and straightforward. Being a part of the Brotherhood helps them obey God, become better Muslims, which, in turn, increases the likelihood of entry into paradise and eternal salvation. This does not mean that members do not care about politics; rather, they may see political action—whether running for a municipal council seat or joining a mass protest—as just another way of serving God.

The tendency to see religion through the prism of politics or economics (rather than the other way around) is not necessarily incorrect, but it can sometimes obscure the independent power of ideas that seem, to much of the Western world, quaint and archaic. For those who no longer see the relevance of religion in everyday life, it can be difficult to understand how people are able and willing to do seemingly irrational things in the service of seemingly irrational ends. But, looked at another way—if we do our best, as analysts, to put aside secular bias—what could be more rational than wanting and seeking eternal salvation?

The dramatic rise of ISIL is only the most striking example of how liberal determinism—the notion that history moves with intent towards a more reasonable, secular future—has failed to explain the Middle East’s realities. Of course, the overwhelming majority of

Muslims do not share ISIL's rigid interpretation of religion, but that is not the most relevant question. ISIL, after all, draws on, and draws strength from, ideas that have a broad resonance among Muslim-majority populations. They may not agree with ISIL's interpretation of the caliphate, but the notion of *a* caliphate is a powerful one, even among more secular-minded Muslims. One of the few surveys on attitudes towards a caliphate (well before the rise of ISIL) found that an average of 65 per cent of respondents in Egypt, Morocco, Pakistan and Indonesia agreed with the objective to "unify all Islamic countries into a single Islamic state or caliphate[16]". This transcended ideology, with even a majority of nationalists saying they supported a caliphate[17].

A way out?

The role of religion in public life has become the primary political cleavage in much of the Middle East (although it overlaps, to various degrees, with economic, class and even linguistic cleavages). Party systems are products of a country's particular history. Over time, they become entrenched and self-sustaining. What happens at the start of the democratisation process is not incidental, nor can it be easily reversed. This is what makes transitional periods particularly tense and polarising. Yet, transitions in the Middle East, whether successful or failed, have proven more polarising than the norm.

> *The tendency to see religion through the prism of politics or economics … is not necessarily incorrect, but it can sometimes obscure the independent power of ideas that seem, to much of the Western world, quaint and archaic.*

At this juncture, cleavages along religious, identity and ideological lines are unlikely to recede to the background. If anything, they have solidified in Egypt and Tunisia and intensified in Libya and Turkey. In Syria and Yemen, ideological cleavages have also grown in importance, although the picture there is somewhat more complicated due to long-standing sectarian tensions between Sunnis and Shias. Yet, in all of these cases, and in all of their diversity, the divides in question are *foundational*—having to do with the nature, meaning, and purpose of the modern nation-state.

Going forward, the best-case scenarios—which would require inclusive national reconciliation processes, the (re-)incorporation of mainstream Islamist parties and a conscious move towards consensual democracies that restrain executive power and distribute power away from an over-centralised state—are simply not possible in most Middle Eastern countries (the two partial exceptions being Turkey and Tunisia).

If anything, the drivers that the author has identified in this paper may produce further destabilisation, particularly in the absence of a clear, strong and coherent vision of the Middle East from the United States and other Western powers. A key variable is whether the divide between pro- and anti-Muslim Brotherhood blocs on the regional level—mimicking domestic polarisation—eases or intensifies. As Saudi Arabia focuses considerable attention and resources on the war in Yemen, their rift with the Brotherhood will likely either remain as is or perhaps further diminish. With this partial exception, though, it is difficult to identify scenarios in which significant improvements are likely in the short run.

A key variable that impacts any discussion of what might, or might not, happen in the next two years or more is the role of the United States. The overarching premise of the Obama administration's approach to the Middle East was what some have termed the Responsibility Doctrine: stepping back to allow others to step in. The idea, here, was to encourage Arab allies to rise to the responsibility and take ownership over their own affairs. Others did, in fact, step in, but in a way that encouraged the worst instincts of regional actors and engendered proxy wars. The US desire to limit its involvement in the Middle East has produced a sense of uncertainty and even panic in the region, which, in turn, has exacerbated regional divides (whether Shia vs. Sunni or Islamist vs. anti-Islamist). The question, then, is whether this posture will persist after the Obama administration, or whether there will be a course correction, in which renewed US leadership—and importantly the perception that the US is renewing its commitment to the region—mitigates the existential tenor of regional competition.

Conclusion

It can be challenging to imagine the ways in which the Middle East can further deteriorate, considering how dire things already are.

But it is worth remembering that this is what many observers also thought in 2013, and then in 2014. One example is a conversation this author had with a friend in early 2012, wondering how many people needed to die in Syria before the US and its allies intervened militarily (by establishing no-fly and no-drive zones, for example). The author suggested 15,000 casualties. At the time of writing, four years later, more than 250,000 Syrians had been killed.

Two of the less obvious countries worth following are Egypt and Tunisia. While Tunisia is successful in relative terms, the prospect of more terror attacks could provoke authoritarian measures in the name of stability and undermine confidence in a fragile democracy. Egypt, meanwhile, is another good example of the difficulty of imagining genuinely worse scenarios. Egypt has always muddled through, despite suffering from troubling economic and political indicators for much of the post-independence period. It has had the fortune—and misfortune—of a strong state. There is a fascinating and troubling debate within the Muslim Brotherhood about the use of ‘defensive’ violence—including burning police cars, the targeting of security personnel who have committed crimes against Brotherhood members and economic sabotage. Yet most of these discussions have remained at a theoretical level, with little actual follow-through from Brotherhood members. If anything, the surprising development is not how many Islamists have turned to violence in Egypt, but how few. For now.

Beyond specific country cases, the shifting landscape within the world of political Islam is already proving to be one of the most important developments of the post-Arab Spring era. For the first time, the Muslim Brotherhood, long the largest and most influential of Islamist movements, has been eclipsed by those on its right flank. In any number of ways, this is the Salafist-jihadist moment, not just in the sense of greater media impact or the ability to influence Western societies through terrorism, but because they are beating the Brotherhood at its own game. The Brotherhood can no longer as easily claim to be more ‘practical’ or better at governing and providing services than Salafist and Salafist-jihadist competitors. However, it goes even deeper than this. In contrast to the ‘vanguard’ model of political change, the starting assumption of most mainstream Islamist groups has been that mass sentiment and support mattered and that the ‘Islamic project’ was doomed to fail without that popular foundation. Even

Al-Qaeda, contrary to popular perceptions, was (and is) quite concerned with how ordinary Muslims perceived it, which was one of the reasons behind the tensions between Ayman al-Zawahiri and Abu Musab al-Zarqawi, over the latter's brutality and wanton killing of civilians, including Shia worshippers.

Yet, ISIL has demonstrated that a relatively small number of ideologically-committed individuals—even ones that go to the furthest extremes of brutality and alienate the vast majority of fellow Muslims—can capture, hold and govern territory, in a way that very few other Islamist groups ever have.

The failures of mainstream Islamist groups, and particularly the Egyptian Muslim Brotherhood, have also re-focused attention on the question of what it means to win. Even more successful Islamist parties, such as the Justice and Development Party (PJD) in Morocco, may be in power but their ability to change or transform society and politics is inherently limited due to the dominance of the monarchy. Meanwhile, in Pakistan, Jamaat-e-Islami, one of the few mainstream Islamist groups that hold on to a more vanguard model, repeatedly loses elections, garnering less than 10 per cent of the vote. They are not particularly popular, yet they are arguably more influential than the PJD through their ties with the military and other state institutions and their role as a kind of sharia lobby which is able to shape the contours of public debate on key issues of concern.

This, then, is yet another consequence of the emergence of ISIL: a shaking of the fundamental assumptions of Islamist movements, which had been locked into a predictable pattern in the previous decades: form political parties, focus on elections, and gradually work to reform state structures from within. These may be good things in theory, but they do not appear to have worked.

CHAPTER 3

Russian futures to 2018

Chapter 3 – Russian futures to 2018

Pessimism characterises much Western analysis of Russian futures. One prominent report suggests that Russia faces "mounting internal difficulties, including a weakening economy and a political climate that stifle enterprise and society". Such problems, the report continued, "imperil both security in Europe and stability in Russia". Necessary reforms face "daunting political obstacles", while the influences that have dragged the Russian economy into recession are "structural, conjunctural and geopolitical" and "market pressures and external conflict pose additional challenges of uncertain duration". If the country "continues its current course—in both economic management and international relations—this will be increasingly dangerous for Europe and costly, if not disastrous for Russia". Indeed, the report went so far as to say that the "new [Russian] model is not sustainable and Western governments need to consider their responses to various scenarios for change[18]".

In Russia the prognosis is also pessimistic, though some points of focus are different. Economists note that if the economy stands at a cross-roads, there is a 45-50 per cent probability that the future will bring a “frozen economy”, in which Russia has a "semi-closed, stagnant economy" with ageing technologies and an ever greater concentration of resources in the defence industry, ultra-high concentration of property, nationalisation, de-industrialisation and low growth rates. According to Yakov Mirkin, head of the department of international capital markets at the Institute of World Economy and International Relations, the next most probable outcome, with a 30-35 per cent likelihood, is a “controlled chill”. This is a slightly more sophisticated version of the frozen economy, which includes "rescue teams" of young technocrats introducing certain elements of modernisation[19].

In broader terms, the consensus appears to be that the future is alarming. Russia’s struggle for its place in the world has not finished, one Russian futures analyst has suggested, as a result of Russia’s position between European, Middle Eastern and Eastern civilisations—and if Russia’s civilisational border with the East is more or less clear, it is in constant movement to the West and South, where foreign powers constantly attempt to increase their spheres of influence at Russia’s expense[20].

Some note that developments in the world have been so "many and so turbulent lately that one can expect every year to bring a revolution or a major change in the global balance of power". This year will hardly be an exception, Fyodor Lukyanov, research director of the Valdai discussion club, has argued: the reconstruction of the world order that began at the beginning of this decade will continue to gather momentum, characterised by chaos, until the new order emerges by 2030[21]. The "major mega-trend in global politics", Sergei Karaganov suggests, is the "war of all against all" in the Middle East. Furthermore, the sharp escalation of the conflict between Russia and the West has led to increasing talk of the possibility of a new war—which some say is inevitable—and the re-emergence of the nuclear issue[22].

In attempting to adapt to the difficulties of imagining the future, most Russian futures analysis focuses on scenario planning as a means of stepping beyond the immediate problems of the day and reflecting on alternative possible outcomes, including possible black swans or wildcards, as they look a decade ahead. This paper, however, will offer short-term foresight of Russia in the period to 2018. In this case, foresight can be usefully based on analysis of longer-term mega-trends, the structural context in which developments take place, and the relative certainties in specific themes that are unlikely to change greatly over the comparatively short timeframe. These mega-trends provide definition of possible futures. The paper will focus on three mega-trends: economics, domestic politics and the international environment. Woven into each mega-trend are game-changers, developments that can affect the course of events within these broader definitions. Game-changers can be both active, in terms of how policy-makers are making conscious attempts to influence the course of events, and passive, including external, often unpredictable developments. Together, analysis of mega-trends and game-changers serves to frame themes to guide foresight, based on extrapolation from more tangible evidence.

Specific predictions about Russia in 2018 cannot be made with confidence. But the contextual trends are very clear, since they are both structural and emphasised by the Russian government's explicitly repeated active game-changers, and thus less likely to be significantly altered even by adverse events. Indeed, adverse passive game-changers may serve to emphasise them.

The shorter timeframe brings into sharper focus some of the major questions being debated in Russian futures analysis. But it also means that some of the questions central to most discussion about Russian futures are not addressed in depth. First, the Russian government consistently attempts to engage in long-term planning, both in wider terms, but also in specific technical areas. During the last decade, numerous strategies framing the period to 2020 have been published, and discussions to plan a strategy to 2030 are well underway. Though it is outside the remit of this paper, this commitment provides the background to some of the active game-changers driving the mega-trends discussed below.

Reform of the economy away from its reliance on hydrocarbons is not at the centre of the analysis. The Russian government has made its timeframe explicit. The Russian Energy Strategy to 2030 sets out a three-stage development plan, and only in stage three, from 2022 onwards, is the shift to the “economy of the future” envisaged. Thus the Russian policy-making community "expects oil and gas to remain the locomotive of growth not only in energy but in the national economy broadly until 2022". Only gradually will the relative importance of fossil fuels decline. This also relates to Russian plans to diversify its energy trade. The energy ministry has stated that the main task is to speed up entry into Asia-Pacific markets, but only by 2035 will all energy exports to Asia reach 23 per cent.

Russia’s demography is another often central theme to futures analysis. The steep population decline since the 1980s, combined with low fertility and an ageing population, has long-term negative ramifications for the economy and military, and, given higher rates of fertility among Russia’s Muslim population, the ethnic mix of Russian society. If most of these problems will be felt only in the next decade, two points nevertheless warrant mention.

First, the government’s long-term family development and transport policies have shown some signs of success. Life expectancy increased to 71 years in 2013, and fertility rates increased from 1.3 children per woman in 2006 to 1.7 in 2012. Demographic data suggests that the decline in population was reversed in 2012, and 2013 saw the first positive increase in natural population growth since 1991. Serious health problems continue, but mortality resulting from transport accidents, murder and suicide have substantially declined.

Second, though Russia has a high rate of emigration, it is also the second largest immigration nation. Some 300,000 immigrants arrive in Russia every year on average, approximately 50 per cent of whom are ethnic Russians. Much of this immigration comes from within the Eurasian region and has been substantially increased by flows of migration from Ukraine since 2014. Some 2.2 million immigrants arrived in Russia in 2014, 89 per cent from Ukraine, and in 2015 a further 3 million came in, also largely from Ukraine. This is likely to sustain Russian population growth over the period to 2018, even as natural growth begins to decline again due to the sharp contraction of the fertile population.

Mega-trend one—The Russian economy: Slow adaption to adversity

The Russian government enjoys a financial cushion of considerable foreign exchange reserves, including increasing holdings in gold, reaching USD 371.6 billion in January 2016. It also runs a substantial trade surplus. However, 2015 saw a decline in industrial production of 4 to 5 per cent, in retail trade of 8 per cent and in real wages by 10 per cent. Indeed, the economy faces a wide range of problems, from high levels of capital outflow to ageing, obsolete industrial machinery and limited and decrepit infrastructure, which have all contributed to a longer-term slowdown in economic growth that began in late 2011. The combined impact since 2014 of the fall in oil prices (decreasing export revenues[23]), the financial sanctions (reducing access to capital) and economic sanctions (affecting equipment supplies) have compounded these structural problems.

The broad downhill trend in economic growth over the last three and a half years accelerated in 2015, with official statistics suggesting a 3.7 per cent contraction in GDP in 2015. Speaking in January 2016, Prime Minister Medvedev stated that 2015 was "perhaps the most difficult year in a decade for Russia" and the country faced "forceful and synchronised challenges". There is continued pressure on the budget, since the 2016 budget assumes an average oil price of USD 50/barrel and a budget deficit of 3 per cent—but the oil price has remained below USD 50. The Russian government is attempting again to cut back budget expenditure by 10 per cent, and Medvedev has stated that the only protected areas will be Russia’s international obligations, security, agriculture and social policy.

If Medvedev has stated that the stimulation of investment activity and the removal of barriers impeding private money from entering the market are important priorities, the most obvious active game-changer is the Russian leadership's increasingly obvious subsumption of the economy into its wider security concerns, as emphasised in the recently published national security strategy. This is because the Russian leadership is seeking to enhance its self-reliance, both to reduce Russia's vulnerability to external measures and increase its ability to act as an independent state. This has led to emphasis on state control of key strategic sectors, the prioritisation of import substitution and the implementation of shadow systems to replace the SWIFT international payment system if necessary. It has also led to shifts in organisational structures, such as the establishment of government commissions to supervise import substitution. More broadly, as the government attempts to consolidate and streamline its budgetary resources, the finance ministry's jurisdiction was extended in January 2016 to include the federal tax, customs, alcohol and budgetary supervision services. In turn, the Kremlin is increasing its control over macro-economic policy and the finance ministry itself.

> *…the most obvious active game-changer is the Russian leadership's increasingly obvious subsumption of the economy into its wider security concern …*

These measures were being implemented before the sectoral sanctions were imposed by the US and the EU, and the substantial resources and legislation devoted to them suggest that it is a long-term policy. While the Russian economy is more open and integrated with the global economy than before, the potential for at least the partial reversal of either domestic liberalisation and international integration is also much greater. This trend faces numerous obstacles—not the least one being a lack of consensus across the economic block and a lack of focus—and as a result, success in measures such as import substitution to 2018 will be uneven, limited to key areas, and likely only achieved more broadly after 2020.

Nevertheless, over approximately the next two years, the state's economic course seems broadly set, tilting Russia's political economy towards security rather than economic freedom, with numerous ramifications for resource allocation and prioritisation, as well as the scope of Russia's external economic activities[24].

Two potential passive game-changers relate to the Russian economy in the coming years, and they are the two most important external constraints on the Russian economy. The first is Western sanctions, and if US sanctions are likely to remain in place for longer, it is probable that the EU's sanctions on Russia for their part will be lifted at some point before 2018. While disagreements over the implementation of the Minsk II agreements remain a sticking point, senior European leaders have begun to voice their objections to maintaining the sanctions. Vladimir Putin has also stated that he is certain that, sooner or later, "normal relations" with the EU will be re-established.

More important is the oil price, which is perhaps the least predictable game-changer, depending as it does on many interlocking factors[25]. There is an ongoing debate in Russia about potential oil price fluctuations. If some see low oil prices as the "new normal", others see a tightening in the oil market by late 2016, which could lead to a slight price increase, towards USD 50 to 60 per barrel. The Central Bank of Russia's (CBR) baseline scenario, for instance, envisages a stabilisation of the price of approximately USD 50/barrel to last for the period 2016-2018[26]. Either way, the predicted rise in this time frame is not considered likely to be substantial.

In the context of the longer-term mega-trend and active game-changer of the government's deliberate securitisation of the economy, neither of these "passive game-changers" are likely to alter substantially the broad trajectory of Russia's economic development. Instead, the economy is more likely to slowly adapt to the adverse environment. The CBR suggests that while the economy is gradually adapting, it needs another year to adjust to negative external conditions. In all its scenarios, external financial conditions will continue to constrain the growth of the Russian economy over the period from 2016 to 2018, though their impact will "gradually abate". Thus the CBR's baseline scenario suggests continued GDP contraction in 2016 of -0.5 to 1.0 per cent, moving firmly into positive territory in 2017 with growth of 1.5 per cent to 2.5 per cent in 2018[27].

Mega-trend two—Russian domestic politics: Consolidating the system

The Russian domestic political landscape is dominated by Vladimir Putin's leadership team and, in parliamentary and regional terms, the United Russia (UR) party, which has held the majority of seats in parliament and the huge majority of regional governorships for over a decade.

The leadership team dominates the strategic heights; however, the Russian governance system is often dysfunctional. Systemic mega-trends in domestic politics are therefore shaped by three factors: the long-term continuity in the Russian leadership team, the leadership's consistent struggle to shape strategic planning and invigorate the bureaucratic system, and an electoral cycle during this period. Parliamentary elections are scheduled for September 2016 and presidential elections in 2018.

Active game-changers will be visible in two ways. The first relates to the election cycle, which will be guided by the leadership's search for wider stability. While support for United Russia (UR) dropped in the parliamentary elections of 2011, it has subsequently consolidated its position and appears likely to benefit from the introduction of a mixed electoral system in which half of the Russian parliament's 450 members will be running on party lists, and the other half on single mandate, independent constituencies. The precise balance of the next parliament's make-up will depend on how this legislative change affects support for UR[28], how much the Communist Party of Russia, which remains the only substantive opposition across Russia[29], can attract a protest vote, as well as the role of the All-Russian Popular Front (ONF)[30].

This sense of imposed stability will be enhanced by the leadership's concern about anything that looks like a potential Colour Revolution in Russia, as well as the extensive measures that have been put in place to prevent that from happening. These measures range from the curbing of external support for Russian NGOs and civil society to legislation to prevent mass demonstrations, to the preparation of the Interior Ministry (MVD) to cope with outbreaks of civil disobedience (as demonstrated by the Zaslon-2015 exercises, explicitly framed by the MVD as preparing to deal with a "Maidan-type" situation).

The second relates to the combination of the make-up of the leadership team and the attempts to increase the effectiveness at all levels of the Russian bureaucratic system. In the coming years, there is likely to be a slow evolution of the team as it seeks to adapt, and as younger members of the elite position themselves for promotion. The age of many of the most senior officials means that there are likely to be retirements[31]; this is likely to be supplemented by the leadership moving officials aside if they are unable to bring the required results. There will therefore likely be an ongoing slow rotation as well as recruitment and promotion of officials.

Two particular passive game-changers may contribute to the political context in the next two years: social protest and terrorism, but on current evidence, neither is likely to substantially alter the broader mega-trend. Since the protest demonstrations in 2011-2012 faded away, there has been little political protest; there have, however, remained aspects of social protest, such as the health care protests in November 2014, and the more recent long-haul trucker protest. These have been limited in scale, however, and have not gained wider public support—or led to a substantive change in government policy.

> *…it is not clear that a successful terrorist attack would substantially alter the political environment or Russian foreign policy.*

Similarly, the threat of terrorism in Russia, from both the North Caucasus and international jihadism, is substantial. But the Russian government has implemented robust, not to say brutal law-enforcement measures against terrorism over the last decade and poured money into attempts to address the problem. Furthermore, given the experience of terrorist attacks in the past, it is not clear that a successful terrorist attack would substantially alter the political environment or Russian foreign policy. Russia has suffered numerous major terrorist attacks, from Nord-Ost to Beslan, from bombings on the Moscow metro and at Domodedovo airport, and, most recently, the bombing of the Russian airliner in Egypt in November 2015. Yet none of these have altered the wider political context.

Over the coming years, therefore, despite potential influences, the push and shove of political life, and some contradictions within the system, the main trend in Russian domestic politics is one of evolving consolidation. Active game-changers will continue to influence the political mega-trends more than visible passive game-changers throughout this period.

Mega-trend three—Russia on the world stage: Assertion in an unstable world

The broad contours of Russia's foreign policy have remained consistent for some time and are unlikely to change dramatically in the next two years. The Eurasian space remains a priority and the Russian leadership has sought to cultivate its position as a hub in the region with the Collective Security Treaty Organisation and the Eurasian Economic Union. China is another priority, and the Russian leadership has for over a decade sought to improve its relationship with its neighbour to the east. This has resulted in an ambiguous but burgeoning economic and security relationship, with major energy and arms deals being signed. Despite these deals, and although this is indeed a priority, it is most likely to come to full fruition after this decade.

> *...the main trend in Russian domestic politics is one of evolving consolidation.*

Although Moscow sees Western influence in international affairs to be in strategic decline and that of Asia as increasing, it is with the West that the main issues will arise in the near future. Long-term contextual trends are visible here, too. Russia's relations with the Euro-Atlantic community began to stagnate in the mid-2000s, and, despite the most recent "reset" of 2009-2012, they have been deteriorating for years. The war in Ukraine only served to highlight the range of disagreements between the Euro-Atlantic institutions (particularly NATO and the EU) and Russia. While Russia retains more positive relations with some member states, many of the mechanisms for multilateral relations have been suspended.

The prospects for Russia's relationship with Western institutions therefore appear ambiguous. There are strong lobbies, particularly in continental Europe, who seek to stabilise relations with Russia—and, as noted above, the Russian leadership has also stated its belief that Russia's relationship with Europe will return to some form of "normality" sooner or later. Thus it may be that over the next few years, EU sanctions are lifted and dialogue is resumed at different levels as the parties attempt to move beyond the Ukraine crisis.

Nevertheless, the war in Ukraine has left a deeply negative mark in both the Euro-Atlantic community and Russia, and the accelerating deterioration over the last five years has been based on fundamental disagreements over many issues ranging from the US withdrawal from the ABM treaty in 2002 and the US-led invasion of Iraq in 2003, to concerns about US-led regime-change operations and the West's rejection of Moscow's initiative to draw up a new European security treaty in 2009-10. There are clear policy disagreements between Russia and NATO over a number of issues—both long-term, such as NATO enlargement and the missile defence programme, and those heightened by the war in Ukraine, such as the permanent basing of NATO equipment and forces on the territory of member states in Eastern and Central Europe. All of these issues are likely to remain serious points of contention and, most immediately, at NATO's Warsaw summit in summer 2016. The Alliance will endorse further enlargement (Montenegro), probably missile defence (the Readiness Action Plan) and possibly other related measures. The tension between the desire to move the relationship beyond Ukraine and these fundamental disagreements will dominate, exacerbated by differences within the communities, but the policies set in motion in both NATO and Russia will reflect the increasing competition between them.

As noted above, however, the main thrust of Moscow's international policy is not related to specific bilateral or even regional priorities, but driven by the desire to enhance Russia's self-reliance in international affairs. This is the main mega-trend. The broad consensus among expert observers and officials alike is that the world is entering a period of considerable turbulence and insecurity, partly as a result of both Western regime change operations, and partly as a consequence of increasing competition between states over resources and values—competition that may result in the outbreak of war. These concerns drive two important themes in Russian foreign and security policy—the need to be able to defend Russia against a possible strategic strike in the mid-to-long term, and the need to be able to project power.

This underpins the active game-changer: the leadership's programme of major military reform and investment in the wake of the Russo-Georgia war in 2008. Since 2010, the leadership earmarked 20 trillion rubles (approximately USD 640 billion at 2010 exchange rates) for the modernisation of the Russian armed forces by 2020. The plans envisage half a million military personnel under contract and ensuring that 70 per cent of the armed forces' weapons are modern. This includes the acquisition of 400 intercontinental and submarine-launched ballistic missiles, 20 attack submarines, 50 combat surface ships, 700 modern fighter aircraft, and more than 2000 tanks and 2000 self-propelled and tracked guns. After a sluggish start, and despite high levels of corruption and ongoing technical problems, these reforms and investments are bearing fruit. Russian officials have stated that by the end of 2015, 30 per cent of weapons were new (more in some areas) and this should reach 50 per cent by the end of 2016.

Furthermore, Russian ground forces have undergone constant exercising at all levels over the last five years, emphasising command and control and combat readiness. The command and control aspect is noteworthy, as a new National Defence Centre was opened in late 2014, the hub from which Russian military operations are being conducted. The exercises have addressed the quality and quantity of equipment and servicemen and were about fighting large-scale interstate war. By 2015, therefore, a Swedish observer has suggested that the Russian armed forces had become "most likely capable of launching large-scale conventional high-intensity offensive joint inter-service operations, or (…) to put it simply, to conduct big war-fighting operations with big formations". Furthermore, each of the exercises during this period demonstrated ambitions to increase Russia's military power, and were conducted in coordination with other agencies, suggesting that the focus was not just the fighting ability of the armed forces, but improving the state's capacity to wage war[32].

Even if defence spending faces possible cuts[33] and some of the re-armament programs are being postponed into the early 2020s, by 2018 (and again by 2020) the Russian armed forces will be transformed, with new equipment increasingly available and combat lessons learned from exercises in Ukraine and Syria.

Additionally, the Russian leadership is investing heavily in bolstering both its strategic deterrence and the defences of both the Crimean peninsula and the Arctic, increasing its military capacity in these areas and its ability to respond to emerging threats. This is changing the strategic landscape.

This is the issue on which passive game-changers such as the evolving tension with Turkey and the situation in Syria can have most effect, since conflict can spin unpredictably. But two points are worth making. First, although much Western attention has focused on so-called hybrid warfare, which has emphasised the informational and special services aspects of Russian power, it is Russia's conventional warfighting capacity that is most notably evolving over the next few years. Second, the primary disagreements and tensions are evident and the Russian leadership shows little sign of softening its position, even under economic duress. Quite to the contrary: Russia has become more involved in Syria to seek to prevent the collapse of the Assad regime; in the wake of Turkey shooting down the Russian bomber in late 2015, Moscow responded not by changing course, but by reinforcing it. Of all the mega-trends, this is the one for Western audiences to watch most closely: it is what drives the subsumption of the economy into security concerns and the attempt to consolidate the Russian state and society.

Russia in 2018

"More of the same" is an unfashionable and, given the tense and uncertain international environment, risky conclusion for a foresight paper. This is perhaps especially so for Russia, when the majority of Western observers have spent much of the last twenty-five years looking to the future with hope for change. Since 2011, Western observers have persistently hoped to see the end of the Putin era, asserting that Putinism was unsustainable; that economic pressures would oblige the Russian leadership to soften and reform the Russian domestic and international position; or that it would otherwise face a popular revolution or an elite split or coup to overthrow the president. In this way, some observers had expected ("liberal") change in Russia as illustrated first in their view by the protest demonstrations in 2011-2012.

The two main passive game-changers are fluctuations in the oil price and tension spinning into conflict with unpredictable consequences. But on the evidence available, and given the relationships between, on the one hand, the economic, political and international mega-trends, and on the other, the active game-changers of Russian government policy, evolving continuity over the next two years is the most probable course of events for Russia. Smaller, day-to-day, passive game-changers will play a role, but they are unlikely to alter substantially the overall direction of Russia’s development.

> *…it is Russia’s conventional warfighting capacity that is most notably evolving over the next few years.*

Thus change over this short period is most likely to be evolutionary, taking place either within the system or at its fringes. These may include the evolution of the leadership team, slight fluctuations in the make-up of parliament and a continuation of fringe social protest. The economy—burdened by structural problems that would take longer than three years to reverse even in favourable conditions, and even if desired by the leadership—faces a period of adaptation, perhaps with a return to some slow growth (within the overall trend of a longer-term slowdown) if oil prices increase. Changes in the economic situation are more likely to be driven by the government’s security agenda, designed to protect Russia against external instability, than by reform towards more liberal efficiency.

The main direction of Russian foreign and security policy is likely to remain consistent: numerous long-term disagreements with the Euro-Atlantic community (even if some are temporarily patched up with continental Europe); attempts to block and prevent the collapse of regimes both in the former Soviet area and in the Middle East and North African regions, which may lead to greater tension with some states (such as the US and Turkey); and the development of relations with China. Such issues are encapsulated in the broader thrust of Russia’s foreign policy when attempting to secure its interests in a period of international instability and to defend its interests abroad.

CHAPTER 4

Weapons of mass destruction: The evolution of the threat of proliferation

Chapter 4 – Weapons of mass destruction: The evolution of the threat of proliferation

The term weapons of mass destruction (WMDs) was coined to reflect modern means of mass destruction. The phrase first appeared in a 1937 *London Times* article about the bombing of Guernica. Its first political use was in a declaration issued by Truman, Attlee and King on November 15, 1945, which called for an international commission to be set up for the elimination of "atomic weapons and all other major weapons adaptable to mass destruction" (meaning biological weapons, according to the drafters). It later appeared in the first resolution of the United Nations (UN) General Assembly (January 1, 1946), which mentioned "all other major weapons adaptable to mass destruction". In August 1948, a UN commission gave the term a more specific technical definition: "atomic explosive weapons, radioactive material weapons, lethal chemical and biological weapons, and any other weapons developed in the future which have characteristics comparable in destructive effect to those of the atomic bomb or other weapons mentioned above".

For legal, strategic and technical reasons, the concept of WMDs currently covers very different issues. In this text, WMDs refer to chemical, biological, nuclear and radiological (CBRN) weapons, as well as to ballistic missile delivery systems with a range greater than 150 kilometres (the threshold used by the Missile Technology Control Regime). These delivery systems may be used to launch either conventional missiles with a powerful politico-strategic effect, including sowing terror, or missiles carrying NBC weapons. This is close to the definition that was used in UN Security Council Resolution 687 (April 8, 1991) regarding Iraqi programs after the Gulf War.

The concept of proliferation is generally understood to mean a horizontal increase in these capabilities, i.e. an increase in the number of WMD possessors, whether they are state actors or non-state actors (such as the Aum Shinrikyo sect, which possessed chemical and biological weapons). The term vertical proliferation, which is sometimes used in nuclear non-proliferation circles, is based on a different rationale. Actors can acquire NBC or ballistic capabilities in three different ways: the creation of a program; a deliberate transfer from one actor to another; or the dispersal of capabilities following the collapse of a state.

There is a solid international consensus that proliferation is dangerous. The acquisition of NBC or ballistic capabilities can foster an arms race, embolden an actor that feels protected by its ability to issue threats of mass reprisals, and affect crisis stability. If such capabilities are put into use, in addition to the obvious immediate humanitarian consequences, it is likely to affect the taboo or tradition of non-use which is present in the nuclear and biological fields.

The current situation and anticipated situation out to 2018 with regard to proliferation must not be exaggerated. In the past 10 years, a number of countries (including Middle Eastern countries) have voluntarily or involuntarily renounced their WMD capabilities or ambitions. Concerns for the coming years centre on about 10 countries. In terms of capabilities acquired, the names that appear the most often in open sources are, in alphabetical order, China, Egypt, India, Israel, North Korea, Pakistan, Russia and Syria. The use of WMDs is limited, in modern times, to chemical weapons and ballistic missiles: it has been many years since the last significant use of biological weapons or, of course, of nuclear weapons.

Proliferation-regulating mechanisms are unlikely to change substantially between now and 2018. Aside from the instruments that are already known and in force (including the Treaty on the Non-Proliferation of Nuclear Weapons, nuclear-weapon-free zones, the Chemical Weapons Convention and Biological Weapons Convention, and the Missile Technology Control Regime), it is doubtful that political conditions will change to the extent of allowing, for example, the entry into force of the Comprehensive Nuclear-Test-Ban Treaty (CTBT), the signing of a Fissile Material Cut-off Treaty (FMCT), the negotiation of a verification protocol for the Biological and Toxin Weapons Convention, the establishment of a WMD-free zone in the Middle East, or the establishment of new nuclear-weapon-free zones.

However, the spread of technology is expected to continue, creating fears of new risks of acquisition in the short or medium term. Increases in trade flows, the multiplication of information distribution channels, and population movements (students, interns, expatriates) all facilitate the dissemination of knowledge and capabilities. One determining factor in counter-proliferation will be the approach used to adapt control regimes and surveillance methods to a constantly changing world. Another determining factor governing the proliferation supply will be the stability of states that currently possess WMDs, since the destabilisation or collapse of such states could put stockpiles, technologies or expertise on the market.

On the demand side, the key determining factors will continue to be regional balances, military (particularly Western) intervention, and relations with those states that provide security assurances (primarily the United States), as well as the nature of political regimes (given that, all other things being equal, liberal democracies today are less inclined to acquire such weapons than other regimes). Perceptions of the new US leadership (President, Congress) elected in November 2016 will be an important parameter. The possible use of WMDs in the period under consideration will also be a vital determining factor: mass use could either reinforce the taboo or tradition of non-use, particularly if the international community reacts strongly, or contribute to making the use of a given WMD commonplace.

Between now and 2018, the countries that warrant special monitoring (acquisition, transfer or use) will be Saudi Arabia, China, North Korea, Iran, Pakistan and Russia.

Nuclear capabilities

Nuclear proliferation is somewhat more predictable than the proliferation of other types of capabilities. Nuclear technology evolves more slowly than chemical or biological weapons technology and requires a greater and generally more visible investment. There are few innovations in this field. The only major developments concern the dissemination of methods and expertise. Centrifuge enrichment techniques were widely disseminated by the so-called Khan network in the 1980s and 1990s (allegedly together with more or less complete weapon blueprints). Laser enrichment, a highly discreet technique, could become popular among nuclear candidate states. However, the transition to nuclear energy in certain countries will lead to the development (still limited by 2018) of civilian nuclear complexes and therefore to basic knowledge in that field.

Apart from Iran, no other country today is publicly known to have both the capability and the desire to acquire nuclear weapons in the near term. However, the issue of Iran will no doubt be a determining factor in the future of proliferation leading up to 2018.

> *Laser enrichment, a highly discreet technique, could become popular among nuclear candidate states.*

The Joint Comprehensive Plan of Action of 14 July 2015 unquestionably represents a turning point in the Iranian nuclear crisis, which has been going on since the existence of secret facilities was publicly revealed in the summer of 2002. However, this agreement, which is essentially intended to prevent Tehran from acquiring a nuclear weapon in the next 15 years, in no way represents a definitive resolution of this matter. Between now and 2018, three scenarios are possible: a) Iran willingly implements the JCPOA and apparently abandons all military nuclear ambitions; b) Iran tries to keep its options open and possibly extract new concessions from the P5+1[34] and tests the resolution of the international community, for example by obstructing access to certain sensitive sites; and c) a major crisis leads to a breakdown, the P5+1 attempt to re-impose sanctions, and Iran resumes its nuclear program. Scenario b) is the most likely.

> *...this agreement, which is essentially intended to prevent Tehran from acquiring a nuclear weapon in the next 15 years, in no way represents a definitive resolution of this matter.*

In all scenarios, this agreement in no way eliminates the risk of nuclear proliferation in the region. First, although Saudi Arabia has officially ratified the agreement, it has concerns about developments in US policy, which it finds too weak or too favourable to Iran. Second, since the agreement legitimizes the possession of uranium enrichment capabilities, it will be easy for other states to demand the same treatment and to refuse any limitation on their uranium enrichment and/or nuclear reprocessing capabilities.

The failure of the Nuclear Non-Proliferation Treaty Review Conference (spring 2015) does not in itself entail new risks of proliferation. However, some Middle Eastern states could, in more or less good faith, use the standstill in the process for establishing a WMD-free zone in that area (the issue that caused the Review Conference to fail) to justify a military nuclear program.

In the Middle East, as elsewhere, US policy will continue to be the most important determining factor in the future of nuclear non-proliferation, second only to the behaviour of Iran. US policy plays a role in three different ways. First, US military interventions serve as reminders of the country's superiority and are the reason that the idea that the only way to protect oneself from the United States is to acquire nuclear weapons has been commonplace since the end of the Cold War. Second, as has been the case since the 1950s, the credibility of the protection that Washington confers on its allies—its formal and informal security assurances—is a key consideration for countries contemplating a potential military nuclear program, particularly Turkey, Saudi Arabia, Japan and South Korea. (Egypt is a special case: it does not have a security assurance from the US but is dependent on Washington for its military budget.) Third, the political relationship that the US has with non-allied nuclear states (China, Russia), as well as with Pakistan, may have an impact on the willingness of those states to share certain technologies.

Saudi Arabia is without question the state of greatest concern. It is the only country today that seems to have the motivation, financial means and adequate bilateral relations (with China and Pakistan) to modernize its ballistic systems and acquire, within a relatively short time, the necessary technology base to contemplate a military nuclear program in one form or another. The evolution of the Washington-Riyadh-Islamabad triangle bears close watching, whatever the reality of current rumours that Pakistan has allegedly already granted a potential nuclear assurance to Saudi Arabia. That being said, the likelihood of a break in the politico-strategic ties between Washington and Riyadh within the timeline under consideration remains low, as the strength of those ties has been tested many times in the past 70 years.

In the coming years, only a few countries are likely to deliberately transfer sensitive (dual-use) nuclear technologies: North Korea, China, Iran, Russia and Pakistan. The first is a special case, as it has actually stated its willingness to deliberately carry out such transfers. The others currently have a restrictive policy in this regard (at least officially), ostensibly so that they can effectively control exports of dual-use assets and technologies.

There is a risk of non-deliberate dispersal in the event that one of those states becomes destabilized or collapses. Again, North Korea is a possibility. The precedent of Syria showed that the risk of such dispersal does indeed exist: the Al-Kibar site was successively occupied by the Free Syrian Army and the Islamic State of Iraq and the Levant (ISIL). The fate of all of the substances, materials and technology related to the Syrian nuclear program is unclear to this day.

Regarding the risk of use, if 70 years without a wartime nuclear explosion can be considered a tradition of non-use, the risk remains very low, but the probability is far from nil in Asia. Despite Russian leaders’ current rhetoric, it is extremely unlikely that Moscow would deliberately use nuclear weapons: Putin is playing the nuclear card to show off his strength, but Russia has not lowered the threshold for using nuclear weapons and has no plans to enter into a direct military confrontation with NATO. The primary risk between now and 2018 is undoubtedly the possibility of an Indo-Pakistani crisis degenerating into an uncontrolled escalation. Although mutual deterrence has limited the risk of a direct conflict between the two countries, a major new attack against India could force New Delhi to react. If the two actors then become unable to control the spiralling violence, Islamabad could be driven to the extreme of considering limited use of nuclear weapons in an attempt to put an end to the conflict, for example by trying to involve the international community. For its part, North Korea, which in 2018 will have acquired the capability to fit nuclear weapons on to mid-range missiles (and perhaps also on basic intercontinental missiles), will remain a great concern given Pyongyang’s proclivities for dangerous provocations.

The acquisition of a nuclear device by a non-state actor remains extremely unlikely. In the event of the sudden collapse of a state such as Pakistan or North Korea, the intervention of external actors to prevent such a scenario would at least partially address this eventuality. As for the risk of access to nuclear weapons stockpiles in Europe – by activists, not by terrorists – it appears not to be high despite a few episodes of facilities being penetrated. If by chance this scenario should occur, it remains to be seen whether the actor in possession of the device would be both willing and able to use it.

Other capabilities

In contrast to the nuclear field, technology evolves quickly in the chemical and biological fields, as shown by micro-reactors in the former case and breakthroughs in molecular biology and genetic engineering in the latter. The chances of state or non-state actors gaining access to chemical or biological weapons during the period under consideration therefore seem far less remote than for nuclear weapons[35]. In the future, the possibility of such weapons being carried by sophisticated drones will have to be taken into account.

> *The chances of state or non-state actors gaining access to chemical or biological weapons during the period under consideration therefore seem far less remote than for nuclear weapons.*

Since the weapons are discreet and the technologies considered are very often dual-use, major uncertainties remain today with regard to the existence of chemical and above all biological military capabilities. Generally speaking, North Korea, Egypt, Syria and Iran are the states of greatest concern. However, China, Israel and Russia, among others, may at least have capabilities that could be militarized quickly.

Biological capabilities

Biological weaponry is the field for which the greatest uncertainties persist with regard to the existence of militarized capabilities or capabilities that could be militarized quickly. Concerns primarily centre on China, North Korea, Egypt, Iran and even Russia.Since 1945, there have been extremely few known instances of biological weapons being deployed for operational or terrorist purposes. In the former case, the last known precedent dates back to the 1970s (Rhodesia). In the latter, the last known instances are the attempted use of botulinum toxin by the Aum Shinrikyo sect (1990s) and the anthrax crisis (2001).

The risk of dual-use capabilities being acquired by many state actors is very high. The likelihood of a state launching a new biological program during the period under consideration appears to be low, although surprises are possible (such as the discovery, in the 1990s, of the unsuspected scope of the Soviet and Iraqi programs). However, non-state actors are likely to attempt to acquire such weapons on a small scale.

The risk that biological weapons could be used in a conflict is extremely limited, owing to the lack of operational value and the scant precedent. The only exception may be North Korea, which is known to be willing to take strategic risks, but it is difficult to imagine this happening, other than in extreme circumstances, for example if the regime felt that its existence was in peril. However, the likelihood of use by a non-state group is higher. This can include not only religiously motivated groups, but also any other millenarian or doomsday organizations. Another scenario could see a militant group carrying out what they intend as a “demonstration” or “warning.” For example, an “anti-globalisation” or “hypernationalist” group could attempt to demonstrate the alleged dangers of opening up the borders by spreading an infectious agent in an airport, train station or port. The situation could get out of hand.

Chemical capabilities

In recent decades, militarization has been much more intense in the chemical field than in the biological field. It should be noted that until the late 1980s, many countries believed that chemical weaponry could be used for operational (offensive or defensive) or deterrent purposes. Since the development of the 1993 Chemical Weapons Convention, most states that previously had a chemical arsenal have renounced and destroyed their capabilities or are the process of doing so. However, a large number of states have retained some potential in this field. The countries regularly cited in open sources are Burma, North Korea, China, Egypt, Ethiopia, Iran, Israel and Syria.

Although chemical weapons continued to be used in international conflicts (Egypt in Yemen, Iraq vs. Iran) into the late 1980s, the last two known instances are when Iraq and Syria used them against their own citizens. This was undoubtedly no coincidence: these two countries, had developed sophisticated military capabilities in the chemical field, primarily for what they claimed to be a deterrent against Israel. These weapons also proved to be useful, from their leaders’ point of view, for intimidating, neutralizing and terrorizing their own citizens when some rebelled against those in power.

> *…an “anti-globalisation” or “hypernationalist” group could attempt to demonstrate the alleged dangers of opening up the borders by spreading an infectious agent in an airport, train station or port.*

The risk that states could start new chemical weapon programs from scratch remains limited. However, the spread of existing weapons or agents in the wake of the destabilization or collapse of a state is a scenario that needs to be considered (see also the case of Syria). It is a possibility in North Korea or even in Egypt or Iran. Furthermore, as in the biological field, and for the same reasons, the possibility that a non-state group could acquire sophisticated chemical weapons is growing (micro-reactors—see above). After having begun using, like other terrorist groups in the region in the last decade, basic chemical explosives (chlorine), the Islamic State in Iraq and the Levant (ISIL) appears to have acquired the capacity to build first-generation chemical weapons (mustard gas) thanks to its ability to source industrial precursors in the Middle East. This would be a first since the Japanese sect Aum Shinrikyo.

The possibility of a new use of chemical weapons remains relatively high. Note that since the mid-2000s, rudimentary but prohibited chemical weapons (chlorine gas) have been used on several occasions, in Iraq and Syria. Regarding the latter country, it is prudent to remember that Damascus has not disposed of all of its binary weapons and could still use them, particularly in a last-resort scenario, if the regime feels that its existence is under threat. The same reasoning applies for a country such as North Korea. Lastly, the probability of a terrorist group disseminating a chemical agent remains high in the Middle East and must be viewed as a possible scenario in Western countries, too.

Radiological capabilities

Rarely considered as weapons of mass destruction, despite being classified as such by the UN in 1948, “radiological” weapons are designed to cause exposure to high doses of radiation in a variety of ways, including poisoning, dispersal by conventional explosives ("dirty bombs") or by aerial vectors, attacks on nuclear facilities, and deliberate meltdowns.

"Dirty bombs" are easy to make. The most radioactive isotopes (eg cobalt-60, cesium-137 and strontium-90) are present in many industrial and scientific institutions and can simply be attached to a conventional explosive[36]. Fortunately, the effects of such devices on the biosphere would be relatively limited: the larger the explosion, the more widely the material would be dispersed, and consequently the more its radioactive effects would be diluted. No doubt this explains, at least partly, why such attacks have not yet been carried out. It would be not be easy to cause a significant release of radioactivity from a civilian nuclear facility, from either the outside or the inside (with the help of accomplices), whether by setting explosives, hacking computer systems or taking control of a reactor. Plots to attack such facilities have existed since the 1970s, but none have ever appeared serious enough to pose a major threat.

The low visibility of the effects of such attacks (unlike conventional bombs and suicide bombings) and the expertise needed to successfully mount a fatal attack undoubtedly explain why most terrorist groups have been relatively less interested in radiological attacks thus far. Nevertheless, given that radiological sources are relatively easy to access and that Western fears of "dirty bombs" are unfortunately well publicised, it seems fairly likely that attempts to use radiological weapons will be made in the coming years, particularly by doomsday groups. In that regard, ISIL is a particular concern because: a) some of its affiliates have expressed an interest in the nuclear field in general (this was also the case with Al-Qaeda in 2001); b) it has been known to use other weapons of mass destruction (chemical weapons); c) it can mobilise individuals with scientific expertise; and d) it likely has access to radiological sources in the territory that it controls in Syria and Iraq.

Ballistic capabilities

Ballistic missiles (which, by convention, refer here to missiles with a range greater than 150 kilometres) are a special case, because they are not weapons per se but rather delivery systems that can be fitted with conventional munitions or NBC weapons. This capability is one of the main reasons that nearly all states that have acquired or hope to acquire NBC weapons have also invested in ballistics.

The opposite is not true: most states that possess ballistic missiles are not known to have NBC programs. The reasons are largely historical: most of them are states that had acquired Soviet SCUD-class missiles during the Cold War.

A total of 31 countries have ballistic capabilities. Among them, 11 have missiles with a range greater than 1,000 kilometres in their arsenals: the eight states that have operational nuclear arsenals, as well as North Korea, Iran and Saudi Arabia. All except Saudi Arabia have or have had nuclear programs with a stated military aspect.

Ballistic missiles have been used many times in recent decades. However, they were exclusively SCUD-class missiles and were generally used for tactical purposes. The rare occasions on which ballistic missiles were deployed for strategic purposes—particularly for terror—occurred during the Iran–Iraq War and the Gulf War. (This does not include missile tests, which may be intended to intimidate.) The last use of such missiles occurred in 2015 during the Saudi intervention in Yemen: as was the case in the Gulf War, Saudi forces and their allies were unable to completely eliminate this threat, and a number of SCUD missiles were fired.

The proliferation of ballistic missiles highlights three major trends: growing use of solid propulsion (which improves engine reliability); enhanced accuracy; and increased range. For these reasons, and because the ballistic missile remains a symbol of power, its proliferation is a lasting trend. The “supply” of missiles and technologies comes primarily from Russia and North Korea. Whereas Pyongyang’s willingness to export its methods and expertise in this field has long been known, Russia could become a more active exporter in the coming years. The SS-26 short-range missile, which is far more sophisticated than the SCUD generation, could prove to be an excellent “export product.”

> *The “supply” of missiles and technologies comes primarily from Russia and North Korea.*

The risk of acquisition therefore remains high. Since the countries likely to be interested are primarily allies or friends of the United States, its relations with these countries will be a crucial determining factor; Western countries could use their political, military and trade ties as leverage or pressure points.

As for the risk of use, there is a relatively high risk of low-level use (missiles with a range of less than 500 kilometres) in Middle Eastern crises and conflicts. A new, high-intensity open conflict in that region or in Asia could lead to more intensive use, and the risk of mass use of medium-range missiles carrying conventional warheads would be an extreme, unprecedented scenario, unlikely to occur anywhere but in the Persian Gulf or the Taiwan Strait.

Conclusion

For the coming years, WMDs proliferation still seems to be a troubling threat, yet one that may be somewhat less significant than 10 years ago in terms of both acquisition (programs, transfers, dispersal) and use.

With regard to acquisition, China, North Korea, Russia and Iran remain the potential suppliers on which concerns will focus, and Saudi Arabia is a serious candidate. US policy—as well as perceptions of that policy—continues to be a key factor in nuclear and ballistic acquisitions. Prospects for biological and chemical weapons seem to be different: it is primarily a problem of disseminating expertise and technologies, and the possibility that non-state actors may acquire such weapons is non-negligible.

With regard to use, it can be said that there is a fragile taboo surrounding the use of WMDs. Four main risks can be identified: a) the use of conventional ballistic missiles by a state (highly probable); b) low-level use of rudimentary chemical, radiological or biological weapons by a non-state actor (highly probable); c) the use of chemical weapons by a state (possible); and d) the use of nuclear weapons, undoubtedly in South Asia (highly improbable, given that every country with nuclear weapons believes that nuclear force must remain a deterrent, not to be used except in extreme circumstances—but with direct and indirect consequences out of proportion to the hypotheses mentioned above).

In closing, there is reason to doubt the relevance of retaining a category that the collective mindset now associates with the intervention in Iraq (2003), along with all the public mistrust that it engendered.

If the classification had to be redone, a number of options would be possible:

- *weapons of mass terror*, under the category of poisons: chemical, biological and radioactive weapons;[37]

- *weapons of mass effect*, capable of causing rapid death to thousands of people: nuclear, biological and chemical weapons;

- *weapons of mass disruption*, capable of causing social disorder, even in low-level use: nuclear, biological, chemical, radiological, ballistic and cybernetic weapons;

- *weapons of mass destruction*, capable of causing large-scale physical destruction: nuclear, incendiary and thermobaric weapons; and

- *weapons of mass catastrophe*, capable of causing major biological effects on millions of people: nuclear and biological weapons.

In all scenarios, nuclear weapons should receive special emphasis: they are the only weapon that can have a mass effect on both physical structures (blast and thermal effects) and the biosphere (the abovementioned effects and ionizing radiation).

Beyond the period under consideration, these categories could be expanded to include new technical developments, such as directed-energy weapons (high-power solid-state lasers) or even weapons stemming from nanotechnology research.

CHAPTER 5

State power and cyber power

Chapter 5 – State power and cyber power

Rapid developments in the cyber realm have caused governments and non-state actors to reconceptualise their understanding of security in an era of pervasive risk. Below are related trends that the author believes may bear significant influence in this area by the year 2018. Those are followed by an examination of structural changes defining the future of cyber-security beyond that horizon.

The bottom line first

National security, per se

- The United States and a number of other countries have identified cyber-insecurity as the paramount national security risk[38].

- Counter-party risk will be a large fraction of total risk for primary targets both in the commercial sector and in the governmental sector. How this affects outsourcing strategies will depend on publicity around detected breaches[39].

- It was widely argued that the loss of confidentiality around cyber armaments due to the revelations of Edward Snowden was a militarily crippling event. "Never let a good crisis go to waste" meant that those revelations were, in point of fact, the initiator of a broad modernisation of cyber weaponry that is ongoing. One may presume that considerable fruit will be borne by 2018, and that other sovereigns are investing in parallel.

Realpolitik

- The concept of Mutually Assured Destruction, demonstrated for industrial controls by Stuxnet, does not and will not have the capacity to ensure threat-stasis as it did in the nuclear world. The reason is attribution: while intercontinental ballistic missiles have a visible flight path and a limited number of launch-capable governments, offensive software has neither.

- Governmental desire for attribution (of actions) and provenance (of traffic) are likely to be unrequited, but those desires will nevertheless be enshrined in policy such as mandatory geocoding of the Internet and data retention demands greater than at present. The increasing stand-off range of non-contact biometrics could appear in a combined mandate. (Present day: facial recognition reaches 500 metres; iris recognition, 50 metres; and, heartbeat recognition, 5 metres).

- Grey-market selling of exploit code will continue to have governments as the primary clientele.

- Major sovereigns will prevent other major sovereigns' products from being used in some aspects of critical infrastructure. While already evident—Huawei routers in the US v. Cisco routers in China—this will extend to cryptographic gear including any sensor product with hardware-embodied cryptographic code. Industrial espionage will thus rise in importance to nation states, as if it were not high enough already.

Force and use thereof

- Civilian strikeback will remain exceptional and only allowable when a civilian entity is paired with a governmental entity, eg, Microsoft with the US Department of Justice against Coreflood.

- Pre-deployment of cyber weaponry in otherwise non-military positions (devices, networks, etc.) is all but certain. Much of it will be for tactical denial of information service of one form or another, but that is likely to expand into disinformation as soon as sensors assume a place in the critical path for autonomous devices.

- The most substantial cyber-centric crime rings will continue to operate from a small number of sovereign jurisdictions wherein they enjoy tolerance if not revenue sharing.

- Silent failure will continue to dominate important breaches; for those entities able to afford it organisationally, ongoing full-network capture will at least be able to answer "How long has this been going on[40]"?

- Cyber attack detection using behavioural techniques, or anomaly detection against long-term norms for example, will be used with greater vigour and immense side-effects.

Control

- The tendency for democratic regimes to delay meaningful response, and then to over-respond, will be demonstrated by cyber events.

- To avoid decision-making under the influence of adrenaline will be ever harder, as demonstrated by the proliferation of proposals with respect to cryptography put forward in the United States in February 2016. The characteristics of financial high-frequency trading—rapid-fire decision-making by self-modifying algorithms—will begin to appear in other domains, including in government.

- Turning decision-making over to machines will be entirely seductive but safe if and only if that delegation can be withdrawn, meaning that the conditions for operating without that delegation are maintained. Similarly, algorithms derived from machine learning must never be trusted unless the "Why?" of decisions those algorithms take can be usefully examined. (The term of art is "interrogatability".)

- Various baby steps towards algorithmic regulation will take place, for example for traffic management, but none of these will yet be critically relevant to either cyber or national security within the period 2016-2018.

- The skills shortage in cyber security will not be solved. Governmental sectors will remain unable to retain those they have nurtured.

Private sector

- Western societies rely on infrastructure that is privately owned—true today, truer tomorrow. Western governments therefore have no choice but to call on the infrastructure's management to perform actions necessary to national security goals. It seems fair to characterise this extension of governmental duty to private sector firms as "deputising" them, regardless of whether it is against management's will to be so deputised. This was, of course, the story around telephone records at AT&T and other companies, and will be the story soon enough around cloud computing and data handlers.

- Multinational companies will face conflicting demands from governments, likely made more severe by governments' increasing efforts at extra-territorial reach.

- The percentage of personal communications that are encrypted will rise, but more due to supplier actions than to citizen actions; this will distinguish free from non-free states to a degree.

- The information given up voluntarily in social media will be increasingly employed by governmental actors. In non-free jurisdictions, disinformation plants in social media will continue to rise in tactical utility to those jurisdictions' aims. In free jurisdictions, social media will be a substantial component to the clearance process.

Research

- The mismatch between features of IPv4 and IPv6 is likely to be exploited in unforeseeable ways, perhaps beginning with address hopping.

- Robot intercommunication, such as vehicle-to-vehicle between self-driving cars, will become a target of research in forensics. Companies have been formed to ensure forensic success just as companies have been formed to ensure forensic failure.

- Cybersecurity as a science will remain a goal and not an accomplishment[41].

Legal framework

- A place in society for those who opt out of cyber life will have to be protected or else the cyber world will simultaneously increase inequality and conformity; think ADA (Americans with Disabilities Act) but for digital rejectionists. This is not an appeal from some "soft Luddite" faction and requires much debate which will be well underway (but by no means concluded) by 2018.

- Compliance regimes will remain of little protective value even as insurers and regulators demand ever more expensive certifications. Few are the enterprises without cyber-related requirements imposed in these ways.

- End-User License Agreements (EULAs) that deny all responsibility will be challenged. Autonomous vehicles may be where such challenges draw first blood.

- Enforceable guarantees for the integrity of retained information, backstopped by some liability regime not yet designed, will come into existence, perhaps focused first on electronic health records (whose black market price is rising).

Discussion

Projecting from now to 1 March 2018, the raw performance of computing hardware per dollar should triple (Moore's Law = eighteen month doubling). There is a parallel twelve-month doubling time for storage per dollar and a nine-month doubling time for network bandwidth per dollar.

> *In non-free jurisdictions, disinformation plants in social media will continue to rise in tactical utility to those jurisdictions' aims.*

Thirty years ago, you would take your data to where the computing was—a university's central computing facility perhaps. Then inventions made it possible to move the computing to where the data was and every worker came to have something on their desktop with which to do that processing. Now come the twin innovations of virtualisation and software-defined networks, so the distal end is once again a display tool while the data is again where the computing is (only now we cannot tell where the "where" is located). Perhaps the next oscillation will put the computing back to where the data will then reside—in the sensor fabric, per se.

Cyber power mirrors biology's ‘punctuated equilibrium’—long periods of stability separated by short periods of rapid change, occasional plateaus of constancy between which everything changes. What may be happening now, however, is an increase in the frequency of oscillation to the point where plateaus of constancy do not last long enough to consolidate cyber policy. That is unsurprising and now permanent; computing technology is in a positive feedback loop. (As wind strengthens at sea, waves stop getting higher and become closer together.)

All advanced, Westphalian governments are amassing the means to project cyberforce, but for the state's monopoly on the legitimate use of force within its territory to have genuine meaning, cyberspace must be balkanised. With enough interconnections, physical boundaries and cyber boundaries lose all correlation, so states increasingly define cyber-territory by where their subjects go, whether by destination control in the Chinese style or by data control in the EU style.

All cybersecurity tools are dual use, just as are knives or gasoline. The US Founding Fathers who wrote "[W]henever any Form of Government becomes destructive..., it is the Right of the People to alter or to abolish it" also wrote "[T]he right of the people to keep and bear arms shall not be infringed", and they wrote both statements in the US constitution at a time when the weapons of the yeoman farmer were on par with the weapons of the infantryman. In the intervening centuries, weapons of infantries so surpassed those of the yeomen that any right of the people to abolish destructive government could not rely on weapons kept at home, but relative might between state and non-state is today closer than it has been at any time since 1791. This oscillation in the balance of power may be peaking, but never before could a dozen people in their pajamas meaningfully annul the monopoly on the use of force.

Worldwide governmental procurement of commercial-off-the-shelf (COTS) products means that breaking the protections on a domestic target requires the same skills and equipment as breaking the protections on a foreign target. In a sense, dual-use COTS cyber technology is deployed more widely amongst the civilian sector than it is in the military sector.

In the 1980s, the civilian sector caught up with the military sector in the design of survivable communications infrastructure. In the 1990s, the civilian sector caught up with the military sector in the application of cryptography. In the 2000s, the civilian sector caught up with the military sector in the deployment of wide-area scalability. In the current decade, the civilian sector is catching up with the military sector in traffic analysis, and the civilian sector has far more listening posts than does the military sector.

Everywhere the talk is about 'big data' and how much better an instrumented society will be, while the rising generation cares less about privacy than do those now in power. Among the classic triad of confidentiality, integrity and availability, we have heretofore prioritised confidentiality, especially in the military sector. That will not be the case going forward. In the civilian sector, integrity will supplant confidentiality as the highest goal of cybersecurity. In the military sector, weapons against integrity will surpass weapons against confidentiality.

The cumulative effect of the curves for computing, storage and bandwidth is this: in 1986, you could fill the world's total storage using the world's total bandwidth in two days. Today, it would take more than 150 days of the world's total bandwidth to fill the world's total storage, and the measured curve between 1986 and today is all but perfectly exponential[42].

> *In the military sector, weapons against integrity will surpass weapons against confidentiality.*

Moore's Law may have begun slowing. Reason No. 1 is physics: We cannot cool chips at clock rates much beyond what we now have. Reason No. 2 is economics: the cost of a new 'fab' (fabrication) doubles every two years—Moore's lesser-known second law. By 2018 one new fab will be as expensive in inflation-adjusted terms as was the entire Manhattan Project[43].

Cryptographic performance is now a front-and-centre topic. The commercial sector is adding cryptographic protections to an expanded range of products and services; but the design question is whether to improve cryptographic performance with ever more adroit software or to implement it directly in hardware. The latter option yields gains in performance not otherwise possible, but embodiments in hardware close out ‘algorithm agility’ as an option for fail-safe design[44].

Over time, in the desktop and handheld worlds, cost stays constant, performance rises and upgrades dominate. Over time, in the embedded world, performance stays constant, costs go down and devices proliferate. Ergo, the embedded systems space makes the attack surface of the non-embedded space trivial by comparison. Beginning in 1997, regular attention has been paid to the questions of monoculture in the networked environment[45], that is to say when all devices share the exact same structure. For an attacker, this means having to write one and only one piece of malware as it can run everywhere. But is not a deep level of redundancy the best way to ensure resilience? Quoting the US National Institute of Standards and Technology (NIST)'s definition of cascade failure,

> *[R]edundancy is the provision of functional capabilities that would be unnecessary in a fault-free environment. Redundancy is necessary, but not sufficient for fault tolerance... System failures occur when faults propagate to the outer boundary of the system. The goal of fault tolerance is to intercept the propagation of faults so that failure does not occur, usually by substituting redundant functions for functions affected by a particular fault. Occasionally, a fault may affect enough redundant functions that it is not possible to reliably select a non-faulty result, and the system will sustain a common-mode failure. A common-mode failure results from a single fault (or fault set). Computer systems are vulnerable to common-mode resource failures if they rely on a single source of power, cooling, or (input/output) I/O. A more insidious source of common-mode failures is a design fault that causes redundant copies of the same software process to fail under identical conditions[46].*

That last part—that "A more insidious source of common-mode failures is a design fault that causes redundant copies of the same software process to fail under identical conditions"—is exactly that which can be masked by complexity precisely because complexity ensures under-appreciated mutual dependence. In sum, cascade failure is much easier in a monoculture, and, as such, when you deploy a computing monoculture, you are making a fundamental risk management decision that the downside risk of a black-swan event is more tolerable than the downside risk of perpetual inconsistency.

If we opt for monocultures, we had better opt for tight central control, recognising the risks that come with it, including the paramount risk of all auto-update schemes—the hostile take-over of the auto-update mechanism itself. The trend line in the count of critical monocultures seems to be rising and most of these are embedded systems both without a remote management interface and long lived. That combination—long-lived and unreachable—is the trend that must be dealt with, possibly even reversed. Whether to insist that embedded devices self-destruct by some predictable age or that remote management of them be a condition of deployment is the national policy question that is on the table. In either case, the Internet of Things, which is to say network-connected micro-controllers in seemingly every device, should raise hackles on every neck[47].

An advanced persistent threat (APT), one that is difficult to discover, difficult to remove and difficult to attribute[48], is definitively easier in a low-end monoculture where much of the computing is done by devices that are deaf and mute once installed or where those devices operate at the very bottom of the software stack—where those devices bring no relevant societal risk by their onesies and twosies, but do bring relevant societal risk at today's extant scales, much less at the scales coming soon. As Dave Aitel has put it many times, for the exploit writer the hardest part by far is test, not coding[49] and monocultures ease testing. Monoculture is not an initiator of attack, it is a potentiator; it is not an oncogene, it is angiogenesis.

In a world of rising interdependence, APT will not be about the impressive machines; it will be about the little ones. It will not go against devices with a hostname and a console; it will go against the ones about which you did not even know. It will not be something you can fix in any of the usual senses of the word "fix"; it can be avoided only by damping dependence. It cannot and will not be damped by supply-chain regulations. You are Gulliver; they are the Lilliputians.

Fifteen years ago, Lázsló Barabási showed it is not possible to design a network that is at once proofed against both random faults and targeted faults[50]. His conception of a scale-free network is good enough for our planning purposes, and today we have a network that is pretty well immune to failure from random faults but which is hardly immune to targeted faults. Ten years ago, Sean Gorman's simulations showed a sharp increase in network-wide susceptibility to cascade failure when a single exploitable flaw reached 43 per cent prevalence[51]. We are way above that threshold in many, many areas, most of them built-in, unseen, silent. Five years ago, Kelly Ziegler calculated that patching a fully-deployed smart grid would take an entire year to complete, largely because of the size of the per-node firmware relative to the available power line bandwidth[52].

The root source of risk is dependence, especially dependence on the expectation of stable system state. Dependence is not only individual but mutual; not only am I dependent or not but rather a continuous scale is asking whether we are dependent or not; we are indeed *interdependent*. Interdependence is transitive, hence the risk that flows from interdependence is transitive. If you depend on the digital world and I depend on you, then I, too, am at risk of failures in the digital world. If individual dependencies were only static, they would be evaluable, but we regularly and quickly expand our dependence on new things, and that added dependence matters because we each and severally add risk to our portfolio by way of dependence on things for which their very newness confounds risk-estimation and thus risk-management. Interdependence within society is today absolutely centred on the Internet beyond all other dependencies, except climate, and the Internet has a time rate of change five orders of magnitude faster.

Interdependence is likewise present at the individual scale; any pool of synchronised data-stores is as jointly vulnerable to a loss of integrity as is the weakest member of the pool. The Gordian knot of our trade-offs is this: as society becomes more technologic, even the mundane comes to interdepend on distant digital perfection. Our food pipeline contains less than a week's supply, just to take one example, and that pipeline depends on digital services for everything from GPS-driven tractors and drone-surveilled irrigators to robot vegetable-sorting machinery, coast-to-coast logistics and RFID-tagged livestock. Are all the technologic dependency and the data that fuels it making us more resilient or more fragile? Morgan Stanley and The Santa Fe Institute believe that it is the latter. Is it not, then, essential to retain manual means for doing things so that we do not have to reinvent them under time pressure?

The way to think about the execution space on the web today is that the client has become the server's server[53]. You take in Remote Procedure Calls (RPCs) from everywhere and everyone. You are supposed to believe that trust is transitive but that risk is not. That is what Javascript does. That is what Flash does. That is what HTML5 does. That is what every embedded Browser Help Object (BHO) does. The HTTP Archive says that the average web page today makes out-references to 16 different domains as well as 17 Javascript requests per page, and the Javascript on-the-wire byte count is five times the HTML byte count[54]. A lot of that Javascript is about analytics, which is to say surveillance of the user 'experience'. On-the-fly insertion of script code has been shown to weaponise the browsers of innocent bystanders[55].

As Daniel Bilar showed in his analysis of Conficker[56], "attackers and defenders each present moving targets to the other"; that is to say that oscillating advantage is to be expected just as in nature's predator-prey dynamics or in game theory. Why? Because a sentient opponent does whatever he can to exploit your code by way of exploiting the assumptions on which your code is built. Sandy Clark showed that if software security is your goal, then "software re-use is more harmful to software security than beneficial", because a sentient opponent first has to learn how your code works and you help him by re-using components[57]. In short, is it time to give up on software security or to double down the way the Language Theoretic Security Group [LANGSEC] shows us[58]? Do we need more evidence than what LANGSEC, Bilar and Clark, with their collaborators, have given us? Is it time finally to accept Ken Thompson's seminal observation that you can only trust a program you wrote entirely and to act accordingly[59]? At least one NYC bank no longer buys software for that very reason.

A leading software security assessment firm is seeing machine written code of vast sizes that contain apparent vulnerabilities—meaning even machines write 'vulns'. In a relatively recent *Atlantic Monthly* article, Bruce Schneier asked a cogent first-principles question: Are vulnerabilities in software dense or sparse[60]? If they are sparse, then every one you find and fix meaningfully lowers the number of avenues of attack that are extant. If they are dense, then finding and fixing one more is essentially irrelevant to security and a waste of the resources spent finding it. Six-take-away-one is a 15 per cent improvement. Six-thousand-take-away-one has no detectable value.

In "Global Cyberspace is Safer than You Think[61]", Eric Jardine says that cyberspace is getting better, not getting worse, that cyberspace is getting safer, not getting more dangerous. His argument is that to think cyberspace is ever worse, ever more dangerous comes from failing to properly normalise whatever measures of safety you have heretofore used. It is only fair to quote its front matter directly:

> *This paper argues that the level of security in cyberspace is actually far better than the picture described by media accounts and IT security reports. Currently, numbers on the occurrence of cyber-crime are almost always depicted in either absolute (1000 attacks per year) or as year-over-year percentage change terms (50 per cent more attacks in 2014 than in 2013). To get an accurate picture of the security of cyberspace, cybercrime statistics need to be expressed as a proportion of the growing size of the Internet (similar to the routine practice of expressing crime as a proportion of a population, eg, 15 murders per 1000 people per year).*

Jardine demonstrates that the denominator matters, that is, that reporting counts of anything is poorer decision-support than reporting rates and proportions; that counts of events per unit time can only mislead; and, that it is incorrect to talk about how much mayhem there is without talking about how much opportunity for mayhem there is.

Jardine's line of critique is entirely straightforward, and cyberspace is not the only place that such arguments about the validity of inference are taking place. Consider Stephen Pinker's *The Better Angels of Our Nature:*

> *We tend to estimate the probability of an event from the ease with which we can recall examples, and scenes of carnage are more likely to be beamed into our homes and burned into our memories than footage of people dying of old age. There will always be enough violent deaths to fill the evening news, so people's impressions of violence will be disconnected from its actual likelihood[62].*

This is, again, an argument for looking at rates and proportions rather than counts. But in a direct cross, Nassim Nicholas Taleb responded with a paper, "On the Super-Additivity and Estimation

Biases of Quantile Contributions[63]", in which he argues that when a distribution is fat-tailed, estimations of parameters based on historical experience will inevitably mislead:

> *When I finished writing The Black Swan in 2006, I was confronted with ideas of "great moderation" by people who did not realize that the process was getting fatter and fatter tails (from operational and financial leverage, complexity, interdependence, etc.), meaning fewer but deeper departures from the mean. The fact that nuclear bombs explode less often than regular shells does not make them safer. Needless to say that with the arrival of the events of 2008, I did not have to explain myself too much. Nevertheless people in economics are still using the methods that led to the "great moderation" narrative, and Bernanke, the protagonist of the theory, had his mandate renewed.*

And to highlight his central point:

> [We are] undergoing a switch between [continuous low grade volatility] to ... the process moving by jumps, with less and less variations outside of jumps.

Is cyber-security getting worse or getting better? Is there anything we are currently measuring that is leading us to conclude that we are doing the right thing(s) as inferred from measurements of what we believe to be outcomes? Are our inferences confounded with little understood assumptions?

Jardine is correct that the possible event space is expanding dramatically, accelerating in its expansion by all accounts. Part of that is network extent. Part of that is the question of attack surface, per se[64]. When we count events, we are misleading ourselves as to whether we are getting better or getting worse. But does changing the divisor alone really make the correction we need?

There is a power law here, to be sure. Wikipedia's concise reminder is that "Power-laws have a well-defined mean only if the exponent exceeds 2 and have a finite variance only when the exponent exceeds 3; most identified power laws in nature have exponents such that the mean is well-defined but the variance is not, implying they are capable of black swan behaviour". That is our situation—

cyberspace does not have a well-defined variance for what can go wrong, and therefore cyberspace is unarguably capable of black-swan behaviour.

Because the near entirety of commercial Internet usage beyond HTML v4 relies upon Turing-complete languages, the security of these services can never be proven because to do so would be to solve the halting problem[65]. As such, the pinnacle goal of security engineering is no silent failure; it is not and cannot be no failure. For society, then, a state of security is the absence of unmitigatable surprise, not no surprises but rather no surprises that do not have a mitigation within reach.

Elroy Dimson famously suggested that the definition of risk is that "more things can happen than will[66]" and our rate of growth in interdependence is absolutely making the number of things that can happen larger. Unfortunately, complexity prevents us from counting the number of things that can happen, hence Jardine's argument that we divide the number of things that did happen by the number of things that could have happened is correct in spirit but would be irrelevant if our estimate of the number of things that could have happened were to be wrong.

Yet if the denominator is the number of things that could have happened and we severely underestimate that, does not that make the news even better? Taleb says no emphatically; the fat tails of power-law distributions enlarge the variance of our estimates, leading to less frequent but more severe failures. The best one could say is that most days will be better and better, but some will be worse than ever. Everything with a power-law underneath has that property, and cyberspace's interconnectivity and interdependence are inherently power-law phenomena. Many tech executives believe Taleb to be correct[67].

A fat-tailed setting inherently resists prediction, but for that very reason makes prediction ever more compelling to pursue. So we get published predictions. Lots of them. Many of them hedge their bets by phrasing their prediction as a question, but that only invokes Betteridge's Law of Headlines—any headline that ends in a question mark can be answered by the word no.

It is a quandary. Fast change means toolsets for protection always trail the need unless the need can be forecast. Fast change makes forecasts hard if that fast change is one of adding mechanisms, not just scale, to the equation. We have both scale, such as an Internet of Things with a 35 per cent compound annual-growth rate, and mechanism, such as afterthought interconnection of sundry gizmos each with new interfaces. And we have a protection deficit as the curves for data breaches show and the number of security start-ups corroborates—Kleiner Perkins is said to be tracking 1200.

To be deadly serious about cybersecurity requires that *either* we damp down the rate of change, slowing it enough to give prediction operational validity, *or* that we purposely increase unpredictability so that the opposition's targeting exercise grows too hard for them to do. In the former, we give up various sorts of progress. In the latter, we give up various sorts of freedom as it would be the machines then in charge, not us—the Defense Advanced Research Projects Agency (DARPA)[68] is betting on increasing unpredictability. Either way, the lessons learned from the 2008 financial debacle about institutions that were too big to fail have to be applied to entities that are too connected to fail or which have too much data to fail.

Endnotes

Endnotes

[1] See China international reserves and capital flows, 26 February 2016, p. 5; China, non-gold international reserves (12 month change) minus merchandise trade surplus (12 month change), Yardeni Report; http://www.yardeni.com/pub/chinareserves.pdf.

[2] Available at http://www.nias.ku.dk/sites/default/files/l_littrup_-_xi_jinping_interview_and_good_academic_practice.pdf.

[3] Snow's famous book, *Red Star over China*, was translated into Chinese as early as 1938, and he remained in favour with Mao until his death in 1972.

[4] Ma Ying-jeou's opening remarks at a press conference in Singapore on 7 November 2015.

[5] Interview with the author, Morsi administration official, 17 February 2014.

[6] See for example Dennis B. Ross, "Islamists Are Not Our Friends", *The New York Times*, 11 September 2014; and Henry Kissinger, *World Order* (New York: Penguin 2014), pp. 121-2.

[7] Wael B. Hallaq, *The Impossible State: Islam, Politics, and Modernity's Moral Predicament* (New York: Columbia University Press, 2013).

[8] For more on the process of Islamist moderation, see Shadi Hamid, *Temptations of Power: Islamists and Illiberal Democracy in a New Middle East* (Oxford University Press, 2014).

[9] The group is known under various names, including Islamic State in Iraq and al-Sham (ISIS).

[10]"داعش يدعو المصريين "للجهاد",” Youtube clip, 29 December 2013, https://www.youtube.com/watch?v=GFsrJADJkqY.

[11] "They shall by no means harm you but with a slight evil", Al-Furqan Media, August 2013; https://azelin.files.wordpress.com/2013/07/shaykh-abc5ab-mue1b8a5ammad-al-e28098adnc481nc4ab-al-shc481mc4ab-22they-will-not-harm-you-except-for-some-annoyance22-en.pdf.

[12] Andrew F. March and Mara Revkin, "Caliphate of Law*," Foreign Affairs*, 15 April 2015.

[13] Will McCants, “Interview: How ISIS uses and abuses Islam”, *Vox*, 18 November 2015, http://www.vox.com/2015/11/18/9755478/isis-islam.

[14] Abu Muhammad al-Adnani, “’In Rabbik bi-l-Mursad”, September 2014; English translation available at: https://archive.org/stream/Mirsad_T/English_Translation_djvu.txt.

[15] Author’s interview with a Muslim Brotherhood official, 9 August 2010.

[16] "Muslim Public Opinion on US Policy, Attacks on Civilians and al Qaeda", Program on International Policy Attitudes at the University of Maryland, April 24, 2007; http://www.worldpublicopinion.org/pipa/pdf/apr07/START_Apr07_rpt.pdf.

[17] Douglas M. McLeod, "Support for the Caliphate and Radical Mobilization", START Research Brief, January 2008; http://www.start.umd.edu/sites/default/files/files/publications/research_briefs/20080131_Caliphate_and_Radicalization.pdf.

[18] Giles, K. et al. "The Russian Challenge". Chatham House Report, June 2015. p. 6.

[19] Mirkin, Ya. “Vneshnaya politika v futlyare ekonomike”, *Rossiya v Globalnoi Politike*, 13 January 2016, http://www.globalaffairs.ru/number/Vneshnyaya-politika-v-futlyare-ekonomiki-17921.

[20] Bezrukov, A. “Stsenarii trevozhnovo budyshchevo”, in Rossiya i mir v 2020. Kontoury trevozhnovo budushchevo. Geopoliticheskii prognoz. Moscow: Exmo, 2015. p. 8. Bezrukov is an advisor to the president of Rosneft.

[21] Lukyanov, F. “Raspad ili pereustroistvo?”, *Rossiya v Globalnoi Politike*, No.1, Jan-Feb. 2016, http://www.globalaffairs.ru/number/Raspad-ili-pereustroistvo-17920

[22] Karaganov, S. “2015: Global Tendencies and Russian Policies”, Russia in Global Affairs, No.1, 2016. http://eng.globalaffairs.ru/number/2015-Global-Tendencies-and-Russian-Policies-17976.

[23] This has been somewhat offset by the depreciation of the ruble and the consequent USD/Ruble exchange rate, since production costs are in rubles and export revenues in USD.

[24] Connolly, R. “Security Above All”, Russia in Global Affairs, No.1, 2016, http://eng.globalaffairs.ru/number/Security-Above-All-17981.

[25] These include the impact of (either or both) a drop in Chinese energy consumption and Iranian oil returning to the international market, and the impact of (either or both) a terrorist attack on a major oil installation or transit network or the spread of regional conflict in the Middle East affecting oil supplies.

[26] CBR figures taken from Central Bank of Russia’s Monetary Policy Report. No.4. Moscow: December 2015.

[27] The IMF and OECD broadly concur—with both suggesting a continuing contraction in 2016 of about -0.5 per cent, followed by 1.0-1.7 per cent growth in 2017, and the IMF forecasts a growth of 1.5 per cent in 2018.

[28] Russian observers have noted that if the 2011 elections had been run on mixed lines, instead of proportional voting system, UR’s result would have been better.

[29] This is not to say that it is a viable alternative to the current leadership, but it is the only party that challenges UR, either winning or coming second in regional elections, and defeating UR candidates in Novosibirsk’s mayoral election in 2014 and for the governorship of Irkutsk in 2015. The so-called “non-systemic” non-parliamentary opposition remains divided among itself and lacking in wider public support.

[30] The ONF is a movement established by the leadership to act as an umbrella organisation that serves to co-opt opposition. The ONF may field candidates in areas where the UR candidate is unpopular, thus soaking up opposition.

[31] Since a number of the most senior civil servants are in their mid to late 60s, retirements and health problems are likely to feature more frequently. The death in January 2016 of Igor Sergun, aged 58, is one example.

[32] Norberg, J. *Training to Fight. Russia’s Major Military Exercises 2011-2014*. Stockholm: FOI, December 2015. pp. 61-62.

[33] “Voennie raskhody v 2016 godu budut umensheny na 5 per cent”, *Vedomosti*, 19 February 2016. It appears that a 5 per cent cut may be applied to defence spending in 2016. It is not clear, however, either whether this will not be replaced from other sources, or that inefficiencies cannot be removed.

[34] Group consisting of the five permanent members of the UN Security Council plus Germany.

[35] In that regard, see this notable warning from the US Director of National Intelligence: “The time when only a few states had access to the most dangerous technologies is past. Biological and chemical materials and technologies, almost always dual-use, move easily in the globalized economy, as do personnel with the scientific expertise to design and use them. The latest discoveries in the life sciences also diffuse rapidly around the globe.” James R. Clapper, Director of National Intelligence, Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee, 26 February 2015.

[36] Numerous incidents involving the theft or sale of radioactive elements are reported each year. However, setting aside the large number that are related to fraud, most of the incidents target materials that are only slightly radioactive (eg natural uranium).

[37] See US Code, title 50, chapter 40.

[38] In the case of the US for example, see White House, "Cyberspace Policy Review," 8 May 2009, www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[39] *Ibid.*

[40] Verizon’s Data Breach Investigations Report consistently reports that 80 per cent of all breaches are discovered by unrelated third parties, not the victim.

[41] See NSA's "Science of Security" award, accessed at: cps-vo.org/group/SoS and "T.S. Kuhn Revisited", accessed at: geer.tinho.net/geer.nsf.6i15.txt.

[42] See www.martinhilbert.net/WorldInfoCapacityPPT.html (reflecting Hilbert & Lopez, *Science*: v332/n6025/p60-65) extrapolated to 2014 with concurrence of its author.

[43]"Slowing Moore's Law: How It Could Happen", accessed at: www.gwern.net/Slowing%20Moore's%20Law.

[44] D. Knuth, "Structural Programming with GoTo Statements, *Computing Surveys*’’, vol 6. No. 4, December 1974.

[45] See for example S. Forrest, A. Somayaji & D. Ackley, "Building Diverse Computer Systems," HotOS-VI, 1997, accessed at: www.cs.unm.edu/~immsec/publications/hotos-97.pdf.

[46] See in Internet Archives, High Integrity Software System Assurance, section 4.2, accessed at: hissa.nist.gov/chissa/SEI_Framework/framework_16.html.

[47] See for example Dan Farmer's work on the Intelligent Platform Management Interface. Dan Farmer, "IPMI: Freight Train to Hell v2.01," 2013, fish2.com/ipmi/itrain.pdf.

[48] Dan Geer, "Advanced Persistent Threat," *Computerworld*, 12 April 2010.

[49] Dave Aitel, Founder/CTO, Immunity, Miami, personal communication with the author.

[50] A L. Barabasi and R. Albert, "Emergence of scaling in random networks," *Science*, 15 October 1999, 286 (5439), pp.509-512.

[51] S. Gorman, et al., "The Effect of Technology Monocultures on Critical Infrastructure," 2004, accessed at: policy.gmu.edu/imp/research/Microsoft_Threat.pdf.

[52] Kelly Ziegler, "Grid, PhD the Smart Grid, Cyber Security and the Future of Keeping the Lights On," USENIX, 2010, accessed at: static.usenix.org/events/sec10/tech/slides/ziegler.pdf.

[53] Mitja Kolsek, ACROS, Slovenia, personal communication with the author.

[54] Trends, HTTP Archive, accessed at: www.httparchive.org/trends.php.

[55] "Baidu's traffic hijacked to DDoS GitHub.com", Insight-labs, accessed at: insight-labs.org/?p=1682.

[56] Daniel Bilar et al., "Adversarial Dynamics: The Conficker Case Study", Springer, 2012.

[57] Sandy Clark et al., "The Honeymoon Effect and the Role of Legacy Code in Zero-Day Vulnerabilities," ACSAC, 2010, accessed at: www.acsac.org/2010/openconf/modules/request.php?\ module=oc_program&action=view.php&a=&id=69&type=2.

[58] LANGSEC, See: "The View from the Tower of Babel", accessed at: langsec.org/.

[59] Ken Thompson, "On Trusting Trust," CACM, August 1984, accessed at: cm.bell- labs.com/who/ken/trust.html.

[60] Bruce Schneier, "Should U.S. Hackers Fix Cybersecurity Holes or Exploit Them?", *The Atlantic Monthly*, April 2015.

[61] Eric Jardine, "Global Cyberspace is Safer than You Think: Real Trends in Cybercrime", 2015, accessed at: www.cigionline.org/sites/default/files/no16_web_0.pdf.

[62] Stephen Pinker, "Violence Vanquished", *Wall Street Journal*, 24 September 2011.

[63] Nassim Nicholas Taleb, "On the Super-Additivity and Estimation Biases of Quantile Contributions", Extreme Working Paper series, 11 November 2014.

[64] The Automatic Statistician, Oxford University, funded by Google www.automaticstatistician.com.

[65] The halting problem is a precise formulation in computer science describing the classes of questions for which the answer is that there is no answer. If a problem can be shown to be equivalent to the halting problem, then, like the halting problem, it cannot be answered. These questions are the computer programming equivalent of saying "I always lie": if it is true, then it is not true, and if it is not true, then it is true.

[66] Peter Bernstein, *Against the Gods: the Remarkable Story of Risk*, John Wildy & Sons, September 11, 2012.

[67] Thomas Lee, "Forget Target, Ashley Madison Hacks, a Bigger Threat Looms," *San Francisco Chronicle*, 20 July 2015.

[68] See SafeWare, DARPA-BAA-14-65, accessed at: https://www.fbo.gov/utils/view?id=9e14f2dee9c21ec99f6aa28555662556.