

7 Risks to Watch

Courcy's Intelligence Service - Established in 1934

January 2012

Contents

Introduction	1
1. China's rare-earth monopoly	1
2. The Stuxnet legacy	4
3. Jihad by Internet	6
4. Space debris	8
5. Russia's shrinking population	10
6. Water	13
7. Solar flares	18

Edited by JKC de Courcy

Introduction

The purpose of this paper is to draw attention to a range of international risks that are given insufficient if any attention in the general media but nevertheless warrant close attention. This is not intended to be a comprehensive list of future risk, but it does provide some thought-provoking analysis and pointers to a number of emerging risk factors to both economic and political stability that are being given insufficient attention.

1. China's rare-earth monopoly

Over the last two decades China has managed to develop what can only be described as a stranglehold on the supply of rare earths critical to the US defence industry.

Rare earth elements (REE) play a vital role in a wide range of electronics and environmental technologies. They are also critical for military applications. The US military uses REE in precision-guided munitions, lasers, communication systems, radar systems, avionics, night vision equipment and satellites. Other off-the-shelf products used in defence systems also require REE, such as computer hard drives. They are not something the military can do without.

The REE are a group of 17 chemically similar metallic elements, comprising the 15 lanthanides and the non-lanthanides scandium and yttrium. The term 'rare' is actually a misnomer, as the REE are quite abundant in the Earth's crust (with the exception of promethium), but they are typically widely dispersed and not often found in concentrated and economically exploitable deposits. REE can be divided into three groups according to their atomic weight and their position in the periodic table of elements: the non-lanthanides, scandium and yttrium; the light REE (LREE) such as neodymium, lanthanum and cerium; and the heavy REE (HREE) such as dysprosium and terbium.

For most of the 20th century REE were sourced from India, Brazil and South Africa, and later the USA. But as demand for different REE has fluctuated, and environmental concerns caused various mines to close, China became the major supplier. China has 37% of the world's proven recoverable deposits, but now produces approximately 96% of the supply, including 100% of the HREE (exact supply percentages are difficult to determine due to the prevalence of smuggling). Total reported world production of rare earth oxide (REO) in 2008 was 126,000 tonnes, a four per cent increase compared to 2007 (121,000

tonnes). World production has more than doubled in the last 15 years, but with consumption of rare earth oxides forecast to reach 190,000–210,000 tonnes by 2015 it is predicted that demand will outstrip supply for certain elements by 40,000 tonnes per year, particularly for neodymium, dysprosium and terbium.

The REE market is more complicated than for many other metals because of the large number of elements, and their broad range of applications for which demand fluctuates over time, largely as a result of technological developments. While prices of other industrial elements have soared in recent years, REE prices have remained low due to the lack of interest in developing mines outside China. But recently there has been growing awareness that precisely because there are only a small number of mines outside China there is a threat to the supply. This threat has become realised as China has begun severely restricting the production and export of REO, and has increased export taxes on all REE to within a range of 15%–25%. Chinese export quotas have been dropping for several years, but the quota slash in 2010, from 50,100 tonnes down to 30,300 tonnes, caused consternation for investors and manufacturers around the world. The final quotas for 2011 were 30,200 tonnes, and although the quotas for 2012 are not yet clear they are expected to be about the same.

Because there are only a small number of mines outside China there is a threat to supply...

Chinese export quota of REO (by thousand tonnes)

2004: 65.6

2005: 65.6

2006: 61.8

2007: 59.6

2008: 56.9

2009: 50.1

2010: 30.3

2011: 30.2

2012: ?

Publicly, China has said that its policy of slashing quotas is driven by the need to improve resource management and conservation, improve the efficiency of resource exploitation, and to protect the environment. But China's actions demonstrate an intention to increase its monopoly and to dominate the rare-earths market for decades. This would also give China control of much of the development and manufacture of vital technology for the rest of this century at least.

The strategy appears to be threefold. The first stage is to limit exports. This year's export quota is likely to be the smallest yet, and there is no indication they are going to increase in the future.

The second phase is to force manufacturers that use rare earths to move to China. Beijing is no longer content to dominate the market as an exporter of raw materials. China already accounts for about 60% of the REE consumed each year, and the plan is to increase that percentage. China wants to retain

as much of the REE as possible, and force the world to buy Chinese manufactured components, thus boosting the economy not only in terms of GDP, but also by increasing education and training to support a manufacturing industry that requires more skilled labour.

Thirdly, China seems determined to control the markets by gaining influence over deposits in other countries. Two Australian companies, Lynas Corp and Arafura Resources, planned to open mines that would have a combined production equal to a quarter of the annual global output of REE. When the credit markets collapsed in 2008 both companies lost their financing. China seized the opportunity and stepped in with the funds and resources required to finish the construction of the mines and ore-processing factories, provided by Chinese state-owned companies. In return the Chinese companies received 51.7% of Lynas and 25% of Arafura.

*China seized the
opportunity and stepped
in with funds...*

Rare earth materials have to go through five distinct processing stages. These are mining, separating, refining, forming and manufacturing. The US used to perform all stages in the REE supply chain, but now most REE processing occurs in China. Industry experts estimate that it will take about 15 years to rebuild a complete US based REE supply chain from mining through to manufacturing. This would require securing capital investment in infrastructure, developing new technologies, and acquiring patents currently held by non-US companies. The US' Department of Defense (DOD) is in the process of assessing the current reliance on REE, and will soon be ready to start taking steps to reduce future dependency, but the need for REE cannot be diminished quickly. Even though a 2010 United States Geological Survey (USGS) study found that the United States had 13m metric tons of REE, the US still lacks deposits of vital HREE. Also environmental concerns have prevented these reserves been tapped, as much of lies beneath various National Parks.

The way forward may be an international approach. Until it closed in 2002, for both environmental and economic reasons, the Mountain Pass mine in California was America's chief domestic source of REE. Mountain Pass is the largest non-Chinese REE deposit in the world, but it lacks the infrastructure to process the ore, and re-developing a complete US supply chain may turn out to be prohibitively expensive. The new owners of Mountain Pass, Molycorp, now plan to fully reopen the mine and ship the ore to Europe for processing. At the beginning of April 2011 Molycorp acquired over 90% of AS Silmet in Estonia, one of only two REE processing facilities in Europe. The move will provide Molycorp with its first European base of operations, and double its current rare earth production capacity to 6,000 tonnes per year. AS Silmet (now to be known as AS Molycorp Silmet) will immediately begin sourcing rare earth feed stock from Mountain Pass.

The Estonian facility, the first of its kind not to rely on rare earth materials from China, will primarily be focused on producing rare earth oxides like didymium metal, a critical component in the manufacture of rare earth magnets. The supply of niobium and tantalum will also be vastly increased.

Has the problem been solved? The answer is probably not. Firstly it is wrong to think of the rare earth marketplace as binary (China/not China). Every country in the world needs REE, so every country, especially those with

domestic REE deposits or processing infrastructure must, first and foremost, serve their own interests. For some of them this will mean dealing with Chinese companies rather than US companies, so China's grip on the global market will not slip completely. Also, even if every other REE deposit were to be exploited China still possesses more than a third of the world's recoverable supply, and so will retain a dominant market position.

Recycling has been hailed as a possibility, and big steps are being taken in this regard, especially in Japan. But recycling REE from, for example, discarded computer motherboards, is an expensive and laborious process. It is unlikely to have a significant long-term effect, and as techniques for recycling improve may even give China another advantage. Chinese domestic usage of REE is skyrocketing, so many of the components available for recycling in the future will be in China.

The only way to escape China's stranglehold on the REE market is to dramatically reduce demand. This will be difficult, as China is likely to do everything in its power to support and develop an industry that provides it with such levers over other countries and other economies.

2. The Stuxnet legacy

The worm is the first malware that actively sabotages industrial systems...

In June 2009 a complex computer virus began to circulate. It wasn't widely recognised, and didn't seem to do much damage. It is now evident that that was an early variant of what came to be known as the Stuxnet worm. By March 2010 an updated version had appeared that was able to propagate more effectively; the third version appeared a month later with some further, minor upgrades.

Stuxnet is unusual in that although it spreads quite easily (due to its ability to exploit more vulnerabilities than any other malware) it does not damage most computers. If the infected system does not meet a very exact set of configuration requirements the virus will not do any harm and will probably go unnoticed. The worm is the first malware (that we know of) that actively sabotages industrial systems. It is also the first to include a programmable logic controller (PLC) rootkit. Stuxnet is carefully targeted to only damage systems that use a Windows operating system; use Siemens PCS 7, WinCC and STEP7 industrial software applications for Windows; and operate one or more Siemens S7 PLCs. This is extremely specific and there are very few systems around the world that the virus could impair.

Iran's Natanz uranium enrichment facility has suffered from a number of setbacks over the last two years, and it just so happens that the installation uses the exact software configuration given above. The effect of the virus is to stop electric motors from shutting down. This was proven by Liam O'Murchu from Symantec, who have analysed Stuxnet, at a conference in 2010; in his demonstration he attached a motor to his computer and programmed it to run for 15 seconds. When the program was run using Stuxnet-infected software the motor continued running indefinitely. There is a significant lack of clarity over Iran's nuclear activities, and it is widely supposed (although denied by Iran) that the nation is pursuing a military nuclear agenda. As

*The media was full of
scare stories about
"another Chernobyl"...*

such, details about the exact problems are hard to establish, but the timeline would suggest that Stuxnet was to blame.

Experts from the Finnish antivirus firm F-Secure have also suggested that the (or at least a) purpose of the virus was to undermine North Korea's fledgling nuclear weapons initiatives.

When the news first came out on 23 November 2010 that PLCs at Iranian nuclear facilities had been infected, the media was full of scare stories warning that Iran could be home to 'another Chernobyl'. The Iranians, by contrast, announced that not only was Stuxnet not a problem, but that there were no problems at all and that the media reports were just western propaganda. In truth, a nuclear accident in Iran (at least one caused by Stuxnet) is highly unlikely, regardless of anybody's rhetoric. The Iranians are not stupid, and they know about Stuxnet. They will be extremely careful not to run infected software, even if it means inventing a different reason to explain delays in their projects.

No-one has claimed responsibility for the construction of Stuxnet, but certain features of the virus indicate that it must have had state backing. Its size and complexity are unprecedented, far beyond anything previously seen. This suggests resources not available to hackers responsible for most viruses. Also, the fact that the targeting of the virus was so specific means that the programmers had to have detailed knowledge of the control systems at the Natanz facility. It has been widely speculated, including by experts like Ralph Langner who first identified the fact that Stuxnet infects PLCs, that the malware was the product of a collaboration between the US and Israel, two of Iran's biggest critics; indeed the conspiracy theory blogs are bulging with references to 'Zionist' words hidden in the code. An article in *The New York Times* in January 2011 made the case for the US/Israeli construction. But in fact there is little hard proof to say who built it. In many ways it is irrelevant. The real threat is that Stuxnet has set a new precedent for conflict. There have been state level cyber-attacks before (or at least via proxies); Russian hackers have attacked both Georgia and Estonia in the past, but they were 'traditional' Distributed Denial of Service (DDoS attacks) in which websites and servers are inundated with more information than they can cope with.

Cyber-warfare provides states and organisations with 'bloodless' ways to attack their enemies, and the burgeoning number of hackers around the world creates the ideal camouflage. The loose association of hackers known as Anonymous, formed in 2003, has been responsible for a large number of controversial DDoS attacks since 2008. It is more likely that this group will grow than disappear, and that their techniques will get more sophisticated; having access to variants of a tool such as Stuxnet, the code for which is now posted openly on hacker websites, could make their attacks more effective. Buried within Anonymous's membership (such as it is) are likely to be a few individuals pursuing more malevolent agendas, and they are going to be extremely hard to spot. As Michael J Assante, former chief security officer at the North American Electric Reliability Corporation, told *The Washington Post*, "Quite honestly you've got a blueprint now, a copycat may decide to emulate it, maybe to cause a pressure valve to open or close at the wrong

A loosely connected series of 'one wolf' individuals.....

time. You could cause damage, and the damage could be catastrophic.”

It is important that IT departments do not adopt a ‘we always know best’ approach to security. In 2009 two hospitals in the UK, one in Sheffield and one in Whipps Cross in London, had system meltdowns due to infection with the Conficker computer virus. The hospitals’ IT departments had decided to avoid installing certain updates, deciding that they were unnecessary, and this allowed the virus to penetrate. This is a particularly apt example. Mikko Hypponen, F-Secure’s Chief Research Officer, believes that Stuxnet could very well be derived from the Conficker worm. In January 2011 he told *USA Today* that he thinks Conficker could even have been the beta-test version of Stuxnet. Conficker was noisy and focused randomly on home and corporate desktop PCs. By contrast, Stuxnet is stealthy and aimed primarily at large factory systems, but uses the same exploit. It is possible that Conficker was used to map network ranges that could be used in Stuxnet attacks.

3. Jihad by Internet

Facebook has more than 500 million users, approximately half of whom log on daily and a billion tweets are sent in a week on Twitter, but who has a presence on these sites? Barack Obama, the British Monarchy, Lady Gaga and Shane Warne have Twitter accounts with thousands of followers. Equally, it is inconceivable that less welcome groups would not have developed a presence on social media sites; the Taliban has a Twitter account and Al-Qaeda has support groups on Facebook.

The structure of Al-Qaeda has changed over the years, moving from an organised pyramidal hierarchy with an ideological and administrative core that directs activities, to splitting these two functions, to a far more loosely connected series of ‘lone wolf’ individuals and small groups around the world with no formal ties to the central organisation, but who draw clear inspiration and occasional guidance from it. One of the principle ways these cells and individuals communicate internally, with each other and with the more traditional parts of the organisation is through the internet, which is proving an especially useful tool in the strategy of mobilising grass root support, particularly in the West.

Islamist ideologues such as Anwar al-Awlaki and Abdullah al-Faisal, both of Western birth, have become key players in the jihad movement through their online activities. Through a deft combination of Islamic teachings, modern pop culture references, and age-old marketing techniques they have established a system to both recruit and radicalise people across the globe without needing them to travel abroad for indoctrination and training – monitoring travellers to particular countries has been one of the key ways intelligence groups have identified potential extremists in the past. As well as reducing the chances of capture, social media has also dramatically shrunk the cost of recruitment.

One of the most important elements of online recruitment campaigns is the distribution of digital copies of speeches and sermons given by al-Qaeda militants, including translated versions of speeches given by members of the

Extremist groups are constantly working to circumvent these restrictions...

core, but these are often buried deep within websites specifically aimed at the already radicalised elements of society, and could potentially remain relatively inaccessible to 'the uninitiated'. In order to draw people towards these resources, mouthpieces have been developed on more widespread social media websites, such as Twitter and Facebook, which can act as a doorway into more serious chat rooms and web forums.

Radical Islamists are not the only ones to have seen the potential in social media. Groups have appeared on Facebook supporting a wide array of extremist activities from far-right to pro-Jihad, although they are often quickly removed from the website. It is worth noting, however, that the number of groups has become too numerous to be individually 'human moderated', and automatic techniques must also be employed to help identify nefarious activity. Extremist groups are constantly working to develop methods of circumventing these restrictions and are increasingly using supposedly peaceful groups as fronts for their real activities. This is not dissimilar to previous tactics of using Islamic bookstores or genuine Mosques to introduce people to the subject, before channelling them towards more radicalising influences. Twitter has not been immune either, with the Taliban setting up its own feed, mainly posting claims for attacks in Afghanistan.

Specific examples of internet-facilitated radicalisation include the Fort Hood shooter Nidal Malik Hasan, who was radicalised through his online contact with Anwar al-Awlaki. Identifiable online influences also contributed to the radicalisation of Umar Farouk Abdulmutallab, the Christmas Day bomber. What is striking about these examples is that both the people who have been radicalised and those doing the radicalising have their roots in the West. It is to be expected that as people in the West become radicalised, or are 'home-grown', they will look to use the tools available to them, and that they are familiar with, to spread their message and further their cause.

There have also been fears that extremist groups are using social media to collect intelligence. The Taliban Twitter feed has been able to access the public profiles of US soldiers and it is not inconceivable that soldiers whose Facebook pages contain information about themselves could have been found by other jihadists. These pages may unwittingly contain images or written information that could provide potential targets for attack. With sites such as YouTube and Facebook allowing people to freely search for topics that interest them it has become increasingly easy for extremist groups to go searching for potential recruits who may be open to listening to some of their more moderate ideas and then slowly feed them more radical ones, rather than waiting for candidates to contact them. Since the recent 'Arab Spring' there has been a lot of talk about the role of Facebook and Twitter in co-ordinating the protests, from all sides of the political spectrum. Extremists are reported to be very interested in how those leading the revolts were able to mobilise and concentrate their forces in a short space of time through social media.

In Al-Qaeda, many of the 'old guard' will be less comfortable using modern technology, but to the 'new blood' it is second nature. However, the new media present a Catch22 for Al-Qaeda. For social media to be used to their

Al-Qaeda's chain of command has become long and unclear...

best effect for recruitment a unified strategy is necessary, but this runs directly counter to the idea of developing a diffuse grassroots movement. The 'administrative core', of Al-Qaeda has been trying to decentralise power so that if a single cell is compromised the rest of the organisation remains relatively unscathed; this type of cell might lack the resources and expertise to carry-out big strikes like the 9/11 attacks, but a large number of small attacks can be equally effective. But a unified web strategy would require precisely the cohesive administration they are trying to avoid. This is also a dichotomy for intelligence agencies. Al-Qaeda's chain of command has become long and unclear, making messages harder to trace back to their source. But equally, Al-Qaeda lacks co-ordination throughout its many affiliates. Social media is seen by both sides as a potential short-cut across large distances and through different cultures, but not an easy beast to tame.

Countermeasures to these new threats are proving tricky to come by; turning off the internet is not an option. Blocking whole websites such as Facebook and Twitter is also not practical; they are currently seen as socially progressive tools that are helping to spread social and political freedom and transparency in developing countries, and extremist groups are increasingly using computer expertise to circumnavigate filters and automated moderators. There are numerous websites that have set themselves up specifically to trawl extremist websites, such as the Nine Eleven Finding Answers (NEFA) Foundation and the Search for International Terrorist Entities (SITE) Group, and suspicious email addresses and exchanges are regularly monitored. This is not a fool-proof method of investigation however, Nidal Malik Hasan was known to be in contact with an identified online recruit, yet no further steps were taken, and investigators failed to connect Umar Farouk Abdulmutallab, who had been reported as a potential threat by his father, to online web posting thought to be his.

It is important to recognise that the basic principles of the methods used by extremists to recruit individuals have not, for the most part, changed; only the manner in which these tactics are brought to bear has altered. Social media have simply allowed extremists to target a new market that they may have previously found difficult to tap. If online recruitment is seen as an entirely new phenomenon, divorced from previous methods, there is a danger that large amounts of resources will be poured into countering the technology, without the recognition that social media exist on a continuum of adaption to new environments that allows traditional methods to still be used.

4. Space debris

With over 50 countries involved in the space environment, it is becoming crowded. This is particularly true of the Lower Earth Orbit (LEO), where many communication satellites, government and private, are to be found. The problem has been compounded in recent years by the proliferation of space debris. Space debris is any piece of material that has been discarded, intentionally or not, that has remained in orbit, rather than returning to earth.

*Eventually there will be
enough space debris
that it will become self-
promulgating...*

For more than 30 years NASA has been predicting that the debris floating in space could form a layer so dense that it would be all but impossible to pass through, leaving us trapped on our own planet. Currently there are more than 20,000 traceable pieces of debris larger than 10 centimetres in diameter, and another 300,000 larger than one centimetre in diameter. It is also estimated that the number of untraceable pieces could number in the millions. Space debris comprises remnants of old satellites, discarded parts of shuttles and various other pieces that have been abandoned in space but have not been pulled into the earth's atmosphere. It is projected that the amount of space debris could triple by 2030 and would continue to increase even if no more satellites were sent up.

A model known as the Kessler Syndrome has been used to predict that eventually there will be enough space debris that it will become self-promulgating, causing a never ending spiral of debris as it collides with itself and is slowly reduced into smaller and smaller pieces. Fears have been expressed that this may already be occurring, and if the amount of debris continues to increase unchecked it could be an irreversible trend. Tracking the debris is a daunting task, and the statistics are complicated. The quantity is not merely physically increasing, but also tracking technology is constantly improving and augmenting the amount of known debris.

In recent years two particular events have dramatically increased the amount of space debris: China's destruction of their own FY-1C satellite in 2007 created over 2,000 new pieces of debris, drawing widespread criticism from the international space faring community; the 2009 collision of Iridium 33, an American communication satellite, and Kosmos-2251, a defunct Russian satellite, the first hypervelocity space clash, resulted in roughly 2,000 new pieces of debris. These pieces have had a serious impact within the LEO, the International Space Station (ISS) has been forced into a number of emergency manoeuvres to avoid pieces identified as having come from these incidents. On 12 March 2011 the astronauts were forced to evacuate to the 'lifeboat' space ship for several hours as a piece of FY-1C passed dangerously close.

One of the reasons space debris has been allowed to flourish unchecked is that there has been little legislation concerned with it. The original Outer Space Treaty lacked the foresight to provide for the problem and there is now little political will to create an international accord that would. A committee has been formed by the leading space faring nations, the Inter-Agency Space Debris Coordination Committee (IADC), to look into the problem, and the topic is regularly discussed at conferences but there remain a number of significant barriers to the process. No one nation wishes to use its time and resources to undertake actions that would benefit all space faring nations without sharing the cost, and an agreement has yet to be reached. Even if there was sufficient political will, there is no consensus on how to solve the problem. Ideas have been proposed that range from building a giant fishing net to equipping a spaceship with a robotic arm to collect the debris, but all seem unfeasible without massive investment and would require international approval. International agreement has been reached with regard to space debris mitigation, with many countries issuing guidelines to minimise the dumping of junk in space, but removal tactics remain unresolved.

The launching state is considered legally responsible for the object during the launch, on-orbit and re-entry phases...

Space debris represents an ever increasing problem to both nations with space programs and to commercial companies that rely on satellite technology, such as telecoms companies. The modern world is highly dependent on satellite communications systems, losing them would be a costly experience for both the companies involved, and their users. Due to the limitations of current launch technology it is impractical to heavily shield satellites and space ships, due to the cost of launching the increased mass (\$9,000 per kilo). Any objects of one centimetre diameter or more in the planned satellite position are considered to pose an operation-ending risk.

Between 2010 and 2013 some 35 satellites will be launched into space, with roughly 25 being insured. Space insurance is, therefore, already a big business, with companies offering insurance against launch failure, failure to stabilise orbit and communication problems throughout the satellites lifespan. Currently most satellites have an 'all risk' strategy that should provide cover, but it remains largely untested and could prove incomplete in the future. Companies are now faced with the very real possibility of colliding with other satellites. This is largely an untested area since no serious collisions between commercial satellites have occurred, and it therefore remains an unknown legal area as far as test cases are concerned. According to the Liability Convention of 1972, the launching State is considered legally responsible for that object during the launch, on-orbit, and re-entry phases and may have absolute liability or fault-based liability for damages caused by the object.

Considering the problems already encountered in tracking space debris, it could be hard to prove liability for small pieces. It is believed that it will also be hard to prove, in the event of two colliding satellites, which one is liable for causing the crash, or whether it would simply be classed as accidental. If the amount of debris does continue to increase as predicted, the cost of insuring space flights could increase in line with the risks, with that cost being passed on to consumers. It is believed, for example, that neither the Iridium 33 satellite nor its Russian counterpart was insured against collision. Russia merely argued that it was not under legal requirement to remove its defunct satellite from orbit, and Iridium's operators may not even have realised that the collision was possible.

Space and satellite technology is a market that has ridden out the recent economic difficulties, actually bucking worldwide trends, and space insurance has grown as a result. Space debris has, therefore, become a topic of major consideration for governments, commercial companies, and their insurers. The potential for a collision is ever increasing and could prove to be very expensive for a badly affected company, losing both capability and customers, whilst having the possibility to render governments blind, ineffective and unaware, impacting on commercial, civilian and military activities worldwide.

5. Russia's shrinking population

That Russia's population is decreasing is a well recognized fact, but potential long term implications are not easy to calculate. Most analysis has concen-

Russia suffers from high death rate, low birth rate, high abortion rate, and a low level of immigration...

trated on the immediate or short term challenges facing Russia, but the consequences for the rest of the world, particularly regarding security, also deserve attention. There are now precedents that could shed some light on what lies ahead.

Preliminary results of the population census, conducted last October, have been published which reveal that 142,905,200 people are currently living in Russia. Official data show that in 2009 Russia saw equilibrium between births and deaths, but despite this, since the last census in 2002, its population declined by more than two and a quarter million from 145,166,700.

Europe as a whole has a higher death rate than birth rate, but Russia is also experiencing other pressures which are not the case for the rest of the continent. The primary causes of Russia's population decrease of about 700,000-800,000 per year are: high death rate, low birth rate, high abortion rate, and a low level of immigration.

Death Rate: Russia has an extremely high death rate of 15 deaths per 1000 people per year. This is much higher than the world's average death rate of just under nine (the death rate in the US, for example, is eight per 1000 and for the UK it's ten per 1000). Alcohol related deaths in Russia are very high and alcohol related emergencies represent the majority of A&E (ER) visits. Russia's high death rate is a particular problem in combination with its low life expectancy. The World Health Organization (WHO) estimates the life expectancy of Russian women at 72 years, but men's life expectancy is considerably lower at only 59 years. This difference is primarily a result of high rates of alcoholism among men.

Birth Rate: Largely due to high rates of economic hardship and alcoholism, women do not feel inclined towards having children. The birth rate in the country is low; the crude birth rate is ten births per 1000 people. The global average is just over 20 per 1000, and in the US it's 14 per 1000. The fertility rate necessary to maintain a stable population in Russia is 2.1 births per woman (the average number of children a woman has in her lifetime), but Russia's total fertility rate is only 1.3 births per woman. Helping to keep the birth rate low is the high abortion rate.

Abortion: During the Soviet era abortion was commonly utilised as a method of birth control; it is a family planning technique that has remained quite popular ever since. Official statistics for the abortion rate cannot be relied upon due to the prevalence of 'back room' abortions, but according to local news sources there are more abortions than births in Russia. They reveal that in 2004, 1.6 million women had abortions in Russia, while only 1.5 million gave birth. And in 2003 the BBC reported that Russia had "13 terminations for every ten live births."

Immigration: Immigration into Russia is low. The immigration that does occur is chiefly a trickle of ethnic Russians moving out of former republics of the Soviet Union. Also, emigration from Russia to Western Europe and other parts of the world is high as native Russians seek to better their economic situation.

The population problem has long been acknowledged at the highest level in

*The brain drain is
compounding the
issue...*

Russia. As Prime Minister (then President) Putin noted in a 2006 speech about birth rates, and about people choosing not to have children: "What has prevented a young family, a young woman, from making this decision? The answers are obvious: low incomes, a lack of normal housing, doubts about the level of medical services and quality education. At times, there are doubts about the ability to provide enough food."

Russia's population is not just declining, it is also aging. The population may be decreasing by up to 800,000 per year, but the workforce is declining by approximately 1,000,000 per year – a state of affairs predicted to continue until at least 2017. The US Census Bureau forecasts that by 2050 Russia's population will have dwindled to just 111,000,000, and 20 years from now there could be just one worker for every 20 pensioners.

But it is not just the birth and death rates that are causing problems. The 'brain drain' caused by the most highly qualified people seeking a better life in the West is compounding the issue. Here is where precedents can be found to predict a possible future for Russia. Conditions in the former Soviet republics of Kyrgyzstan, Tajikistan, Turkmenistan and Uzbekistan are worsening. Even Kazakhstan is beginning to look bleak. When these Central Asian countries gained independence from the Soviet Union they inherited functioning infrastructure, but over the last two decades this infrastructure has crumbled. Insufficient resources were made available to maintain and upgrade the hardware, and inadequate education means that domestically trained engineers are too few and not suitably qualified. What few resources were allocated diminished further due to corruption. As the remaining technicians who are able to keep the systems running die out the future looks uninviting. The countries are sliding, seemingly inexorably, towards failed statehood, and failed states are ideal homes for extremist groups. The worsening situation in Central Asia may not be due to a decreasing population, but it is due to a growing deficit of skills, and this is the same thing that could happen in Russia; whether the skills shortfall is due to a lack of people or a lack of qualified personnel, the effect is the same.

Looking to the future, Lev Gudkov, a demographer with the independent Russian Center for Public Opinion Research said "Whole regions of Siberia and the Russian far-east are already depopulated, and new deserts are appearing even in former 'black earth' regions of central Russia. We will not be able to maintain our industry, agriculture or our armed forces."

Russia's immigration problem is exacerbated by xenophobic attitudes and legislation. Most Western countries compensate for low birth rates by permitting temporary and permanent forms of immigration, which provide both skilled and unskilled workers to keep economies growing and bolster tax revenues. But even since it embraced a more globalised view of economics, Russia has resisted that solution.

"The only acceptable sources of immigrants for us are the Russian-speaking populations of former Soviet countries in the Commonwealth of Independent States [CIS]," says Yevgeny Krasinyev, head of migration studies at the official Institute of Social and Economic Population Studies in Moscow.

"Xenophobia remains very strong..."

This means that a paradox is created where most of the acceptable sources of immigration are countries which are already in trouble due to a lack of qualified personnel, and people from the CIS countries to the west of Russia are much more likely to be tempted to move further west than east. Typifying the problem, Alexander Belyakov, a pro-Kremlin parliamentarian and head of the Duma's Resources Committee, said: "We will encourage people to come from CIS countries, but Russia does not need any other immigrants."

Experts say that Russia not only has no immigration strategy, it has no effective laws to govern the issue at all. "There are only prohibitions," says Viktor Voronkov, director of the St. Petersburg Center for Independent Social Research. "This guarantees that most immigration remains illegal, a boon to only the black market and the criminalized part of society." Mr Voronkov says the main obstacle to rational immigration guidelines is a deep fear of being overwhelmed by outsiders. "Xenophobia remains very strong, not only in the Russian street but at the highest levels of officialdom as well," he says.

The only non-CIS country providing a significant influx of immigrants (albeit mostly illegal) is China, and this is exacerbating the xenophobia issue rather than helping to solve the immigration problem. Russia and China are on generally good terms, but they enjoy a complicated relationship. As we have noted before in our weekly Courcy's Intelligence Brief there are bones of contention, such as Russia's publicly expressed concern over China's arms trade, and China's refusal to recognise the pro-Moscow breakaway mini-states of Abkhazia and South Ossetia in the Caucasus.

We are not suggesting that Russia is going to become a completely failed or pariah state. However, it must be recognised that if Russia's population and workforce continue to decline then there is a very real danger that the authorities could find themselves losing their grip on some regions. If parts of Russia become controlled by extremist or organised crime groups, then those regions could become key launching pads from which terrorists or criminals could launch attacks against anyone they choose with impunity. Since the end of the cold war relations between Russia and the West have improved, but they are delicate, and it is not just the isolationist lobby that would be reluctant to intervene in Russia. There is unlikely to be political or popular will to risk war with Russia, but nor is it likely that Russia will ask for help any time soon. Population decline may first be a threat to the country involved but it is a problem that, sooner or later, will provide challenges for the rest of the world.

6. Water

Water is the most visceral of issues and disputes over water have the capability to cause serious military conflict. This paper looks in detail at one area of dispute: that between India and Pakistan over the Indus. It needs no rehearsing that India and Pakistan are both nuclear armed and nurse deeply rooted animosity towards each other. Before looking at this dispute in depth, however, the following is a selected list of areas where water issued could lead to conflict:

*The visceral issue of
water...*

- Rio Grande/Rio Bravo and Rio Conchos (drought and access to water – Mexico/US)
- Colorado River system (Downstream pollution and water shortages – Mexico/US)
- Grijalva River system (Flooding, pollution, access to water, migration, damage to Malpas dam – Guatemala/Mexico)
- Amazon River basin (Drought, water shortages, deforestation, migration – Brazil/South America)
- Mamore and Beni Rivers (Hydroelectric potential, instability – Bolivia/Brazil)
- Parana River (Dam-induced water shortages – Argentina/Brazil/Paraguay)
- Peru river systems (Contamination, deforestation, mining – Peru)
- Danube River (Hydroelectric potential, water quality – Hungary/Slovakia)
- Kura-Araks River system (Downstream pollution and water shortages in Azerbaijan – Armenia/Azerbaijan/Georgia)
- Sea of Galilee and Jordan River (Water shortages – Israel/Jordan/Lebanon/Syria)
- Lake Chad (Shrinking lake, diminished fishing industry, water shortages – Cameroon/Chad/Niger/Nigeria)
- Nile River (Pressure for additional access, pollution – Egypt/Northeast Africa)
- Lake Victoria (Shrinking lake, diminished fishing industry, water shortages – Kenya/Tanzania/Uganda)
- Okavango River Basin (Drought, access to water – Botswana/Namibia)
- Balkhash Watershed (Cross-border water pollution, water shortages – China/Kazakhstan/Kyrgyzstan)
- Syr and Amu Darya river systems (Glacial melt leading to flooding, water shortages, migration – Afghanistan/Kazakhstan/Kyrgyzstan/Tajikistan/Turkmenistan/Uzbekistan)
- Ganges Delta, Ganges and Brahmaputra Rivers (Access to water, threat to biodiversity – Bangladesh/China/India)
- South Himalayas (Glacial melt leading to flooding, water shortages, migration – South Asia)
- Mekong River (Chinese development policies, access to water – Cambodia/China/Laos/Thailand/Vietnam)
- Salween River (Hydropower potential – China/Myanmar/Thailand)
- Yangste and Huang He Rivers (Flooding, pollution, access to water – China)
- Imjin River/Hwanggang Dam (Flooding, water used as political weapon – North Korean/South Korea).

Pakistan and India: The Indus Water Treaty

The Indus Water Treaty (IWT) of 1960 has recently become a bone of contention between India and Pakistan. While relations are already poor, the breakdown of this accord would signify a new low, and herald the emergence of new security and humanitarian crises on a grand scale.

The Treaty, signed at a relative high point of Indo-Pakistani relations and against the backdrop of water regulation reform in India, sets out which country has the right to access and control the various rivers that feed into the Indus River, and the Indus itself. Since the two countries were largely split along religious fault-lines, rather than obvious geographic boundaries, and part of the River in question is in the still disputed Kashmir region, access to this vital resource has always caused argument between the two.

Despite their differences the importance of the resource, the largest irrigated area of any one system in the world, led to a surprising amount of co-operation, highlighted by the fact that the treaty is still in force and (until now) relatively well respected. This level of co-operation has deteriorated recently, however, with a number of factors putting pressure on both sides and adding to the mutual distrust and political acrimony surrounding Indo-Pakistani relations. Both countries have been rehashing old arguments that have lain dormant for over 50 years, with Pakistan claiming that India has become greedy and is attempting to take more than its fair share of water. India tends to see the IWT as fairly flexible, with changes allowed so long as they are within the spirit of the treaty or which could prove to be mutually beneficial for both countries. Pakistan, on the other hand, tends to be more dogmatic and rigid in its interpretation of the treaty. This is the root of many of the current disagreements.

The key water-use issues comprise drinking water, agriculture, commercial industrial use, electricity generation through hydro-electric dams and navigation. The problems arising from the mutual exclusivity of agriculture and hydro-electricity generation are of particular concern. Hydro-electric dams built upstream, in this case in India, would be able to store large amounts of water behind them in order to ensure a continuous and regular flow. This has the knock on effect of reducing the flow of water further downstream, in this case in Pakistan, thereby reducing the amount of water available for irrigating agricultural land.

Under the IWT India was granted control over the uppermost parts of the Indus River, whilst Pakistan was granted control over roughly 75% of the water. Canals were built from east to west to ensure that Pakistan received all the water it needed. Both parties are required to seek permission from the other to make any substantial changes and a cross-country committee, the Permanent Indus Commission, with representatives from both sides was set up to monitor and resolve arguments. The Commission is currently involved in the resolution of three major disputes, all of which involve Indian Hydroelectric dams potentially restricting the flow of water into Pakistan. The Kishanganga dam row is the first to be referred to international arbitration under the treaty after the two countries failed to come to an amicable agreement. The Kishanganga dispute is of particular importance because

*Another cause for
tension between India
and Pakistan...*

India has planned 33 new dams which have the potential to withhold significant amounts of water from Pakistan..

Pakistan is also vying to construct its own project – the Neelum-Jhelum hydro scheme – on the Pakistani side of the Neelum River. This dam would be rendered significantly reduced in capability if the Indian dam was built above it, and the effect that two dams would have on the flow of the river further downstream in Pakistan is considerable.

Under the terms of the IWT, whichever country manages to complete its building projects first will have priority rights over the rest of the river. Pakistan's projects were initially scheduled to finish first but they have been so beset by internal power struggles and administrative and financial difficulties, whilst (due to its larger and more flexible economy) India has been able to channel extra man-power and resources, that India's projects are due for completion before their Pakistani counterparts. In total, India has planned 33 new dams on its parts of the rivers, which have the potential to withhold significant amounts of water to the agricultural regions of Pakistan during dry seasons or in the sowing period of April-June before the yearly rains come when water is most needed.

Pakistan has cited India's ability to withhold water from its agricultural areas as a major sticking point in current Indo-Pakistani relations, something that India has been keen to dismiss. India has pointed out that Pakistani irrigation systems are woefully inefficient, with as much as 40% of all water being lost before it reaches the roots of plants; also that the UN has awarded it a carbon grant to aid in the building of its dams, something the Pakistani authorities could have protested about before building had even begun, but chose not to. Pakistan is already classed as one of the driest countries in the world, close to falling into the UN's category of 'water scarce' countries, and water availability per person per year has fallen from about 5,000m³ in 1947 to around 1,000m³ today. The majority of this drop has been caused by a large increase in population and a natural decrease in the amount of water coming from the rivers. Recent agricultural trends in Pakistan have also seen a shift towards more water intensive crops such as cotton. Pakistan received upwards of \$18 billion in aid from the US alone in the decade following 9/11, a figure bolstered in 2010 due to the extra aid provided to help counter the devastation caused by the floods. If Pakistan fails to address its agricultural and power issues the amount of aid required could increase dramatically, which would have significant budget implications for developed nations.

India is not in a significantly better position than Pakistan when it comes to abundance of water, with only slightly higher water availability per person per year of 1730 m³, predicted to decline to 1240 m³ by 2030. Agriculture accounts for roughly 90% of water usage in India – expected to decline to 75% by 2050. There is an adequate water supply to meet current needs, but the size of the population is expected to increase dramatically, and even to exceed China's by 2040. India's wheat and rice yield is predicted to drop by 30%-50% by 2050, whilst demand is expected to rise by 20%, meaning that imports, which are currently negligible, will become necessary to the tune of 12.5 million tonnes by 2050, which is likely to push the price of wheat up globally.

At the moment Pakistan is the country being more vocal in its objections to the treaty, while India remains happy with how it has been administered.

Tensions have been running high since the Mumbai bombings of 2008...

This should be seen in the political context of the two countries, with Pakistani politicians keen to stir up anti-Indian sentiment for their own internal ends. It is important to remember that this is merely one strand in a long series of disputes between India and Pakistan. For example, there is unceasing acrimony over the nuclear issue, and tensions have been running particularly high since the Mumbai bombings of 2008. This leads to the question of whether either side, especially Pakistan who are expressing the most anger at developments, has properly considered the effects of the actions it is taking with regard to their water security, or whether they are simply using it as a proxy for more emotive issues.

As well as cross border disputes Pakistan faces an internal water crisis with a large disparity between the Punjab and the Sindh regions. The Punjab region is located upstream of the Sindh and has therefore been able to gain first access to the waters of the river Indus, leaving it little more than a trickle lower down and causing a severe lack of water availability in the Sindh region. By blaming India for 'stealing' its water the Pakistani authorities have been able to overlook this disparity and avoid taking responsibility themselves.

Provided sufficient water continues to flow in from India, Pakistan has the potential capacity to generate much of its required power through hydro-electric dams, with water already Pakistan's third highest source of energy, behind only natural gas and oil. This has, however, been hampered by administrative and infrastructural problems, along with more inter-regional rivalry. Individual regions in Pakistan have taken a position on their own dams, each fearing that large areas may be flooded or deprived of water to provide power to another region. Pakistan's own internal Inter-Provincial Agreement of 1991 has failed and each region is, ironically, expressing similar concerns to each other as the whole of Pakistan is expressing to India. It is illuminating that the Indian Inter-State Water Disputes Act of 1956 is still in force, yet Pakistan's much more recent legislation has already collapsed into bickering and infighting. These disputes have allowed Islamic extremist groups to begin to use water as a 'lightning rod' to stir up dissent.

On a global scale, an outstripping of demand for wheat in India could drive wheat prices up and increase water reliance on the subcontinent. Pakistan faces a serious internal struggle to ensure it allocates sufficient water to each of its regions; failure to do so could cause a humanitarian crisis that would require large amounts of aid to resolve, impacting the budgets of developed nations and potentially creating large numbers of immigrants looking for safer climates. The willingness of first world countries to accept both of these is dissipating.

The current dispute over water between India and Pakistan must also be recognised as just one factor in an always volatile relationship, which could cause further crises in a region that is already unstable. It must also be considered whether either country has accurately assessed the problems they face, or are more concerned with scoring political points, leaving the problem of water scarcity unresolved until it is too late.

7. Solar flares

Most of the world's population has an increasing reliance on modern technology, and a new threat has recently been highlighted which demonstrates a key vulnerability. If something interfered with the power supply to any given area, particularly a large city the consequences could be dire.

An enormous solar flare was recorded at 0156 GMT on 15 February, directed at the Earth. The US space agency quickly recognised that the source of this activity, sunspot 1158, was growing rapidly. The flare proved to be the strongest in four years. The eruption was what is known as an X-flare, the strongest type. This kind of increased activity on the sun can interfere with modern technology on Earth, such as electrical power grids, communications systems and satellites, and satellite navigation systems. Indeed, there is precedent: in 1972 a geomagnetic storm provoked by a solar flare knocked out long-distance telephone communication across the US state of Illinois; and in 1989 another storm plunged six million people into darkness across the Canadian province of Quebec.

Even as recently as 1989 the world was much less dependent on technology. Since then, the advent of the world-wide-web has revolutionised global communications, and the number of satellites in orbit appears to be increasing at a logarithmic rate.

Solar flares and the threat to technology...

Solar flares are caused by an unusual release of magnetic energy stored in the sun's atmosphere. A flare is a sudden, rapid, and intense increase in brightness. A solar flare occurs when magnetic energy that has built up in the solar atmosphere is suddenly released, emitting radiation across virtually the entire electromagnetic spectrum, from radio waves at the long wavelength end, through optical emissions to x-rays and gamma rays at the short wavelength end. The amount of energy released is the equivalent of millions of 100-megaton hydrogen bombs exploding at the same time. Solar flares have been recorded regularly since 1859. Solar flares extend out to the sun's rarefied gas layer, the corona, which normally has a temperature of a few million Kelvin. Inside a flare, however, the temperature typically reaches ten or 20 million Kelvin, and can be as high as 100 million Kelvin.

As magnetic energy is being released from the sun, particles, including electrons, protons, and heavy nuclei, are heated and accelerated in the solar atmosphere. The energy released during a flare is typically on the order of 0.0001027J/s (Joules per second). Large flares can emit up to 0.0001032J/s of energy. This energy is ten million times greater than the energy released from a volcanic explosion, although it is less than one-tenth of the total energy emitted by the sun every second. There are typically three stages to a solar flare: First is the precursor stage, where the release of magnetic energy is triggered. Soft x-ray emission (between 0.12 and 12 kilo electron volts (keV)) is detected in this stage. In the second or impulsive stage, protons and electrons are accelerated to energies exceeding one mega electron volt (MeV). During the impulsive stage, radio waves, hard x-rays (between 12 and 120 keV), and gamma rays are emitted. The gradual build up and decay of soft x-rays can be detected in the third, decay stage.

The trouble with solar flares is that we are not able to predict when they will occur...

The trouble with solar flares is that we not able to predict when they will occur, although we are able to forecast when they are more likely to occur. Researchers say the sun is 'awakening' after a period of several years of low activity; the frequency of flares coincides with the sun's eleven year cycle. When the solar cycle is at a minimum, active regions are small and rare, and few solar flares are detected. These increase in number as the sun approaches the maximum part of its cycle. The danger is that if this current period of high activity passes without incident, other than some unusually spectacular displays of the aurora borealis, then the potential threat will slip back down in the public consciousness as more pressing and immediate issues are dealt with.

If a large flare temporarily knocks out the power to a whole sate, or even a whole country, it is unlikely to cause a catastrophic event. However, a large part of the world's technology, particularly communications and satellite navigation (for cars, planes and ships), functions based on the fact that satellites provide a synchronised time-code. Satellites are not as robust as most ground based technology; they are more exposed to the sun's influence by dint of the fact that they are not at all protected by the Earth's atmosphere, and much less protected by its magnetic field. If they are damaged they may not come back online, and they are much harder to repair or replace.

Shielding critical infrastructure from natural disasters remains high on the agenda; barely a year goes by without a major hurricane, tsunami or earthquake causing an emergency situation somewhere. Solar flares have been hitting the Earth for as long as there has been an Earth, but it is only now we have developed more advanced technology that we have realised they are there, and that they pose a threat. Amongst the planning and threat mitigation that is done to protect from the effects of natural disasters, some resources need to be set aside to study past solar activity as the results could inform the prediction of future space weather, and help mitigate threats to global infrastructure.

Courcy's Intelligence Service - January 2012