The Unexpected Expected- Risks of Tomorrow

Margaret Ross[1], Bryn Parry[2]

[1]School of Media Arts and Technology
Southampton Solent University
East Park Terrace; Southampton, SO14 0RD
Margaret.Ross@Solent.ac.uk

[2]School of Business and Law
Southampton Solent University
East Park Terrace, Southampton, SO14 0YN
Bryn.Parry@Solent.ac.uk

Abstract

The paper discusses the expected and unexpected risks associated with computers, and the financial implications. Past examples are considered, relating to issues of energy, weather and cyber-attack. In greater depth, the increasing risks associated with Fire Ants and the possible latent and unexpected risks associated with Y2K are discussed.

Keywords: Risks, Power Outage, Energy Blackout, Denial of Service, Fire Ants, Y2K legacy

1. Introduction

With it the increased dependence on computing, risks must be considered relating to an expected interruptions, whether resulting from accidental or deliberate technical problems, actions of people, changes of legislation or loss of power. The "cost", not only of reputation and financial cost, can be high, even leading to potentially deadly situations.

Since one can turn to the *World Economic Forum* for a framework of the “Global Risks Landscape 2016” [1], the authors begin by offering a couple of benchmarks, as an indicative context for the scale of impact that the twin-threats explored in this paper might well trigger a risk-cascade towards

1.1 Distributed Denial of Service

Many will recall the *DDoS* (Distributed Denial of Service) that struck Estonia [2], with one researcher noting [3] that: “The severity of the Estonian cyber attacks served as a wake-up call to the world … digitally targeting and nearly crippling the critical infrastructure of technically sophisticated nation-states”. Going on to note that the Estonian state was “… so reliant on the Internet that its model of government operations is referred to as "paperless government” …”

Arbor Networks reported [4] that, in 2015, over 200 DDoS attacks wieldedtraffic volumes of some 100 gigabits per second [Gbps] and that the largest involved some 500 Gbps-equating to the national traffic for Kenya. Regarding commercial organisations, Neustar [5] reported that 32 percent of companies estimate that DDoS would cost over £240,000 per day and that, although UK companies reported being at greater financial risk during a DDoS outage, most still rely on traditional defences such as firewalls - not purpose-built solutions like DDoS mitigation hardware or cloud services.

The BBC [4] notes that *"… there is now a wide range of "booter" services which offer to launch DDoS against specific targets for as little as $10 (£7)"*, quoting John Graham-Cumming [chief technology officer at DDoS protection service Cloudflare]: *"My sense is that DDoS is just part of the internet at this point - it happens … It's a bit like petty crime."*

This not only highlights the scale of impact that the twin-threats explored in this paper might trigger, across a more digitally-reliant city or state than Estonia, but - with those launching such DDoS attacks monitoring their targets for weaknesses, over significant periods - any organisation or state that relies on a critical IT infrastructure that has not definitively rectified any poor Y2K-fixes may not even be aware of the true level of danger that they are exposing themselves to. Even if one avoids the scale of the consequences wreaked upon Estonia, the range of costs from data-loss alone, that Verizon charts [6], could prove terminal for many an organisation.

1.2 Power Outages

The White House "*estimates the annual cost of power outages caused by severe weather between 2003 and 2012 … to have cost the U.S. economy an inflation-adjusted annual average of $18 billion to $33 billion*" [7]

In 2003, a relatively simple event triggered a risk-cascade that saw unprecedented power-cuts right across Italy [with only the island of Sardinia escaping] and the country being, temporarily, divorced from the electricity grids of the rest of the European Union [8].

As the world geared up to meet the perceived threat from Y2K, in 1998, Auckland, New Zealand, was forced to live through the consequences of those disaster-scenarios, when its electricity-supply cables failed and the city's Central Business District suffered a five-week power-outage [9]. The city's main hotels all operated with back-up generators; however, this did not help as worried travellers merely delayed, diverted or cancelled their bookings – whilst many Small and Medium-sized Enterprises failed to survive the longer-term consequences of that five-week spell.

So, if you are tempted to think that the twin-threats being explored in this paper are either far-fetched or have had their potential impacts inflated, please bear these indicative benchmarksin mind, when reading what follows.

2. The Expected Unexpected - Fire Ants

There are risks, which are unexpected currently in Europe but already experienced in countries such as North America. Imported Fire Ants [*Solenopsisinvicta, Solenopsisrichteri*], aggressive types of ant found originally in the jungles of Brazil, have extended their range to such countries as Australia and USA [10]. The mobility of these ant colonies are increasing, by their ability to form "ant rafts" to cross rivers and survive flooding areas. They are able to enter "sealed" areas, and withstand situations that would destroy many other creatures. An example of this is fire ants crawling on food being cooked inside microwave ovens, but not being killed [11]. The computing-related problem is that Fire Ants, apparently, show a strong affinity for electricity, particularly to computers and, by cutting into the cables as well as by short-circuiting connections, thatcan result in a power-out.

These Fire Ants are reported as being attracted to electricity, so in 2010, the BBC [11] reported that "their antennae are electro - sensitive and the ants react to electrical charges by attacking them with their jaws. The Soldier ants, also, like the sweet taste of the terminals and they can't resist having a nibble. All this activity creates problems that leads to dangerous short-circuits as their jaws and legs touched exposed circuitry". Fire Ant actions have long been associated with increased failures of traffic lights [12,13], and with failures of airport landing lights [13,14], even the closure of an airport.

The Taipei Times in 2015 [15] reported that the fire ants not only caused electrical outage at the Taiwan Taoyuan International Airport, but they burrowed under the runways, and are considered "a major threat to aviation safety".
A further risk to airports was reported in 2015, causing a series of five to eight minute closures, relating to birds feeding on Fire Ants nests close to the runway at Vancouver Airport. In 1988, the Pittsburgh Press [13] reported that they chewed "insulated wires and cables, knocking out telephone service, traffic signals and airport landing lights". Various attempts have been made to minimise the activities of the ants, including using coffee grounds at the Charlotte Douglas International Airport in North Carolina [16].

This expected risk is heightened by the global changes in climate. Floods and storms do not seem to stop these ants, while increasing temperatures encourage enlargements of their "territory". This has apparently increasedthe coverage by Fire Ants in the USA. The Fire Ants have reached some parts of Africa and Europe.

Colonies of a different but equivalent electrically-dangerous species of ant were first found within England, in 2009, at Hidcote Manor, Gloucestershire [17] and a nest of these ants has been located in Hendon, London, with more in Buckingham [18].

3. The Unexpected Expected - Y2K Bug

In the preparation for the year 2000, efforts were made to "remove" the Y2K bug which was caused by earlier programmes recording the year with three digits instead of four digits. Programmes were checked and modifications were made to prepare for the eve of 2000. Despite these plans, various aspects of the Y2K bug were experienced at different times [19,20]. Some problems were experienced at predicted times after the first of January 2000, such as at the end of February 2000, depending if the leap year had been correctly programmed. That error also caused problems at the end of December 2000. The issues appeared to re-appear at these dates until the end of 2004, but not publically reported. Nowadays, these problems are widely seen to be over, but there is still a Y2K risk.

Due to the need to complete any changes of coding and full testing prior to 2000, some organisations, in order to "buy time", took the then accepted action of “windowing” or "putting the clock back ". Some organisations used a multiple of 28, being compatible with days of the week and leap years, while it was reported that others such as 50 years were used. This "quick fix" was easy, by subtracting the appropriate number of years, following the calculations, and adding the years to the result. This allowed extra time to fully test the new programmes before replacing the old programmes. Dr Chris Hawkins who took a lead in the UK in assisting organisations to address the Y2K problem, was aware that various organisations used this "temporary fix" [19,20]. Unfortunately there was no legal requirement to record that such an approach had been used and when, or if, the "temporary fix" had been removed.

Warnings about windowing were raised before, during and after the year 2000. Peter de Jager [21] stated that "the whole strategy of windowing (a shortcut Y2K programming technique used by most organisations without expanding data fields to four characters) will come back to haunt us. It has not been documented properly". This technique is safe only if it was formally and officially recorded as a risk, clearly documented and fixed in the short term, ideally prior to any further modification to that system. This technique was believed in 1999 to be going to be widely used. The Associated Press [22] reported in the US that "some government agencies, such as the Social Security Administration, have generally shunned the method. The Inland Revenue Services allow it only rarely. The State Department is using it on nearly half its most important computers, but also plans to replace those systems within five years. Other agencies, such as the Federal Aviation Administration, freely acknowledge using the technique".

With the pressure on delivering computer systems, and the financial crash since 2000, it is more reason to expect that a few organisations could have been tempted to delay the development and testing of the post 2000 replacement system.To simplify the accommodating the days of the week and leap years, some organisations used 28 years or a multiple of this, whereas others were reported to be using 50 years. Even if no modifications to computer systems were made, post introducing windowing, the choice of the years such as 50 created slightly more risks associated with leap years which by-now should have both been exposed. Few computer systems remain "stable" for many years, unless those in authority are unsure about the risks of making any changes. This situation currently exists with some legacy systems.

To exacerbate the situation, since 2000, there have been various takeovers and mergers, resulting in possibly combining IT systems. These in turn could have been using windowing techniques but associated with different numbers of years. Due to the lack of required records, due diligence searches would have been unlikely to identify these issues. The movement and promotion of computing staff, including in many cases the retirement of the relevant staff, who were involved in the various organisations Y2K preparations, would no longer be involved with the computer systems, so delaying the identification and fixing of up the "echo" of the Y2K bug.

4. Risk Context

Senge [23] highlights two aspects of Risk and of Systems that are particularly pertinent to this paper. Firstly, he reminds us to ensure that we have included all of the critical elements of the system that our business is operating within and that "… more often than we realize, systems cause their own crises, not external forces or individuals' mistakes."; individuals "… have it in their power to eliminate the extreme instabilities that invariably occur, but they fail to do so because they do not understand how they are creating the instability in the first place." Secondly, in his "Shifting the Burden" diagrams, he demonstrated how if one only treats the symptoms and does not address the fundamental issues, then a time-delayed side-effect will be triggered that, at some point in the future, will come back and worsen those fundamental issues. The criticality of both of these aspects has been seen, at play, as the twin-threats explored in this paper have been discussed.

Many will be familiar with Risks where the balance of probability and magnitude follows a re-assuring power law curve, some might even be comfortable with "Black Swan" where, as Senge warned against, it was a failure to include an issue or a failure to conceive a possibility that triggers the risk. Arguably, the potential consequences of the twin-threats explored in this paper more closely correlate with Dragon King events [24], where the risk-cascades triggered fall outside power laws, but where greater understanding might not bring individual events into areas of predictability

Hence the call for further research and reflection.

5. Conclusions

Of the twin-threats that this paper has explored:

- regarding Fire Ants, since the lessons from the US are that, once present, eradication is most unlikely, this threat should be moved up the agenda, whilst there is still time - let us not repeat the experience of the Icelandic ash cloud debacle, where time to plan for a known threat was squandered
- regarding Windowing, the generic warnings of Senge [23] were eloquently contextualised by Peter de Jager [21] in that quote: "… the whole strategy of windowing … will come back to haunt us. It has not been documented properly".

It is beyond the space available, in either the conference presentation or in this paper, to adequately communicate effective mitigating strategies; hence, the focus has been on calling for a stronger focus on and further research into the twin-threats of Fire Ants and flawed Y2K-fixes.

6. References

1. World Economic Forum (2016) "*The Global Risks Report 2016*", Geneva, World Economic Forum, 11th Edition [viewed 12/2/16]. Available from: *http://reports.weforum.org/global-risks-2016/*
2. BBC (2008) "*Estonia fines man for `cyber war'* ", BBC News, 25th January [viewed 12/2/16]. Available from: *http://news.bbc.co.uk/1/hi/technology/7208511.stm*
3. Herzog, S. (2011) "*Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*", Journal of Strategic Security, Vol.4 No.2 [viewed 12/2/16]. Available from: *http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss*
4. BBC (2016) "*DDoS: Website-crippling cyber-attacks to rise in 2016*", BBC News, 27th January [viewed 12/2/16]. Available from: *http://www.bbc.co.uk/news/technology-35376327*
5. Neustar (2014) "*Annual United Kingdom DDoS Attacks & Impact Report*", Staines-upon-Thames, Neustar Incorporated
6. Verizon, 2015. "*Data Breach Investigations Report*", Verizon Enterprise [viewed 10/2/16]. Available from: *http://www.verizonenterprise.com/DBIR/2015/*
7. Executive Office of the President (2013) "*Economic Benefits Of Increasing Electric Grid Resilience To Weather Outages*", Washington DC, The White House [viewed 12/2/16]. Available from: *http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf*
8. BBC, 2003. "*Huge blackout cripples Italy*", BBC News, 28th September [viewed 12/2/16]. Available from:*http://news.bbc.co.uk/1/hi/3146136.stm*
9. Wired (1999) "Life In The Dark", Wired, 14th January [viewed 12/2/16]. Available from: http://www.wired.com/1999/04/life/
10. Lard, C.F., J. Schmidt, B. Morris, L. Estes, C. Ryan, and D. Bergquist (2006) "*An Economic Impact of Imported Fire Ants in the United States of America*", Texas A&M University [viewed 12/2/16]. Available from: *https://articles.extension.org/sites/default/files/Copy%20of%20the%20National%20Study.pdf*
11. BBC, 2010. "Swarm: Nature's Incredible Invasions – One Million Heads, One Beautiful Mind", BBC Four, 26th June.
12. New York Times (1990) "*Science Watch*: *Infested Traffic Lights*", New York Times [viewed 12/2/16]. Available from:

http://www.nytimes.com/1990/01/09/science/science-watch-infested-traffic-lights.html

13. Pittsburgh Press, 1988. “Fire ants, supercollider on crash course”, 24th December, p.A17, Pittsburgh: Pittsburgh Press [viewed 15/2/16]. Available from: *https://news.google.com/newspapers?nid=1144&dat=19881224&id=Wt4cAAAAIBAJ&sjid=YmMEAAAAIBAJ&pg=6995,3736485&hl=en*

14. Tschinkel, W.R. (2006) “*The Fire Ants*”, Cambridge, Harvard University Press, [viewed 12/2/16]. Available from: *https://books.google.co.uk/books?id=vxt5BqOKEAIC&pg=PA61&lpg=PA61&dq=%22fire+ants%22+%22landing+lights%22&source=bl&ots=8fVY6WcOt1&sig=a6iiWB1Ia_SmQ8xrP0HWzUh3jLc&hl=en&sa=X&ved=0ahUKEwiKn6XUprTLAhWHXhQKHS3HBwIQ6AEIHDAA#v=onepage&q=%22fire%20ants%22%20%22landing%20lights%22&f=false*

15. Taipei times, 2015. “Beagle trio scour airport for fire ants”, 12th October [viewed 15/2/16]. Available from: *http://www.taipeitimes.com/News/taiwan/archives/2015/10/12/2003629870*

16. WCNC, 2011. “Airport uses coffee grounds to keep ants away”, Charlotte: WCNC [viewed 15/2/16]. Available from: *http://www.wcnc.com/story/news/health/2014/06/28/10742572/*

17. National Trust, 2014. “Asian super ants”, National Trust, 24th July [viewed 15/2/16]. Available from: *https://ntpressoffice.wordpress.com/2014/07/24/asian-super-ants/*

18. Gander, K. 2014. “Super ants with deadly attraction to electricity escape from Gloucestershire and head for London”, London: Independent [viewed 15/2/16]. Available from: *http://www.independent.co.uk/news/weird-news/super-ants-with-deadly-attraction-to-electricity-escape-from-gloucestershire-and-head-for-london-9627259.html*

19. Ross M, Staples G, Hawkins C, 1997. Crisis Management - The Year 2000 problem, Proc Inspire 97, Gottenburg, Sweden 1997., 1997 Process Improvement - Training and Teaching for the Future, 1-899-621-180, IVF

20. Ross M, Staples G, 1997. A Worldwide Software Engineering Problem - The Year 2000 - Will it go away? Proc. Isseu 97, Rovaneima, Finland 1997.

21. Cope, J., 2000. “*Leap Day Skips Past With Few Problems*”, Computerworld, 3rd March [viewed 12/2/16]. Available from: *http://www.computerworld.com.au/article/102795/leap_day_skips_past_few_problems/*

22. Bridis, T., 1999. “*Temporary Y2K fix may last only a generation*”, Athens Banner-Herald, 16th March [viewed 12/2/16]. Available from: *http://onlineathens.com/stories/031699/new_y2k.shtml#.Vr9IvfmLSUk*

23. Senge, P. (2006) “*The Fifth Discipline: the art and discipline of the Learning Organization*”, London, Random House Business Books

24. New Scientist (2013) “*Slaying Dragon Kings could prevent financial crashes*”, New Scientist, 20th November [viewed 12/2/16]. Available from*:* *https://www.newscientist.com/article/mg22029443-000-slaying-dragon-kings-could-prevent-financial-crashes/*