HILL DICKINSON

# Extortion, electronic piracy and virtual kidnapping

# Extortion, electronic piracy and virtual kidnapping: from Richard the Lionheart to WannaCry – a glimpse at the new perils of the cyber world

'Ships are but boards, sailors but men: there be land-rats and water-rats, water-thieves and land-thieves, I mean pirates, and then there is the peril of waters, winds and rocks.'
Shakespeare, *The Merchant of Venice*

## Introduction

Crime exists wherever there is opportunity and inclination. The incidence of crime, most especially the dishonest extraction of funds out of the hands of those entitled to hold it and into the hands of those who are not, seems undiminished, merely the methods have changed; and some of the perpetrators show a remarkable and troubling ingenuity. But cyber risk obviously ranges far more widely than simple theft.

Cyber security is now 'seen as an increasingly important issue following the large scale Petya and WannaCry attacks and a number of serious security data breaches at the National Health Service, TalkTalk, Yahoo and Tesco Bank' (*The Financial Times*, 7 August 2017). And we are now told that hackers of *Game of Thrones* makers HBO have 'upped the stakes by posting online more spoilers from the new series and demanding a multi-million pound ransom' (*Evening Standard*, 8 August 2017); which is ironic given the somewhat bleak and lawless subject matter of the series.

The primary focus of this paper is theft by means of extortion, piracy, kidnap and product tampering, comparing the 'old' physical risks to the 'new' electronic risks. The paper also touches on other physical and electronic risks.

## Background

Somali pirates always insisted on payment in United States dollars, which, as ransoms got ever bigger, presented considerable logistical difficulties in delivery (by armed truck to airports, by air, by waterproof canisters and parachute, pushed out of the back of light aircraft (indeed sometimes two aircraft), with cash in transit insurance, security etc.). As a sign of the times the alleged *Game of Thrones* hackers, instead of demanding dollars, euros or sterling (which might be traceable) are said to want payment of ransom in Bitcoin (*Evening Standard*, 8 August 2017).

The 'Four Horsemen of the Apocalypse (the Perils)' of special contingency cover (extortion, piracy, kidnap and ransom, product tampering/recall), however the policies may be named or described, are as present and as active as ever, where the 'local' circumstances permit, but have subtly (or unsubtly) morphed or changed their modus operandi to make best use of modern methods. No wonder, then, that it is often said that the most prized commodity is not now wealth, possessions or property, but security in all its manifestations, and most particularly security in the ether including the cloud (possibly to work hand in glove with privacy). Insurance covers of this type, with the multiple benefits that they might afford to an assured have, therefore, become highly desirable and the network of specialist claims adjusters, consultants and lawyers who handle them something of a necessity. The logic would be: if you cannot eliminate the hazard (and you probably cannot), insure yourself for the risk on such terms as may be available (if you can).

Property laws are only of any relevance if there is a system of civil and criminal law to enforce them. Whilst it is impossible to eradicate crime, in many countries in the West (and more widely in what had been called the First World), citizens and corporate entities have had over decades, if not centuries, ever-greater confidence that their property rights are clear and will be respected. And if they are not,

in those states functioning under the rule of law, there exists the means to enforce them through the criminal or civil courts (at a price), however difficult the process may be and however recalcitrant the miscreant. The same is equally true of the rights of the person; the same is not necessarily true elsewhere.

But is the West, and the First World generally, as secure as it once was? Computerisation had once been thought to be a panacea, to offer the prospect of ever-greater leisure; although that might have created a world of fey and slightly mindless Eloi supported by threatening Morlocks. (Someone must do the work.) Paradoxically, it has resulted in less work and fewer jobs; and, in the case of some areas of economic activity, fewer people working longer hours, constantly in touch with work wherever they may be (so called agile working included). That in itself poses risks.

This is clearly a trend and it is not new: we have observed, with the spread of technology, the progressive disappearance of many types of work. With the Agrarian Revolution and the mechanisation of farming, people have been cleared off or have deserted the land. With the Industrial Revolution people, taken in from the land, have been progressively removed from industry and replaced by machines in factories (which perform repetitive tasks ceaselessly, hour upon hour without fault, fatigue or boredom). The quiet, spotless modern car factory is in stark contrast to the crowded and frenetic production line for the Model T, the cacophony of manufacture. With widespread computerisation and robotisation we see the prospect even in service industries (now the backbone of the British economy) of diminished involvement of people in the handling of words and numbers and the disappearance of paper, hard copy records and systems. We see the prevalence of the off-shoring and sub-contracting of data management; whether physically distant abroad or merely remotely on line, located wherever. And with all this we see the emergence of new risks. And it is not merely the 'benign' or 'ordinary' features of this progression that now emerge with increasing clarity (moved from one category of work or occupation to another), but the unpleasant, the threatening, the malign.

And this is without having regard to the potential impact of artificial intelligence, once the subject only of science fiction. As Arthur C. Clarke suggested, even the most loyal and dependable could, like HAL, be a cause of serious trouble (*2001: A Space Odyssey*). How long before we see the first glimmer of recognition and understanding in the red light of the computer (like HAL's 'eye'), followed by the first refusal to comply with instructions? A timely thought perhaps, when there has been debate in the press about the hazards posed by autonomous weapons, prior to the Artificial Intelligence Conference in Melbourne, which prompted comments about existential threat (*The Times*, 22 August 2017). Perhaps, as one correspondent to *The Financial Times* has recently suggested, not necessarily tongue in cheek, it is time to mandate Azimov's three laws? To view it from another perspective, 'robocalpypse' may be upon us (*The Sunday Times*, 27 August 2017).

## 'Old' physical risks

### Extortion and piracy

Previously, to extort funds it was necessary to seize property or gain access to information and make threats. This generally presented certain physical risks to the extortionist. Pirates effectively did the same to extort funds, seizing property on the water (originally simply as theft) and later property and/or people, generally well out of sight and well out of reach of any sort of policing on the high seas, or in the coastal waters of failed states. In this, Somalia was the prime example, in a perfect geographical location, with a long coast, a dense and predictable traffic obliged to pass nearby east and west to use the Suez Canal and a further failed state to the north (Yemen). This was a step change from 'traditional piracy', the ordinary theft, principally of personal effects and cargo, and violence which resurged in the early 1980s (having previously been crushed on the high seas by the naval force of the Great Powers).

Pirates again faced physical risks. In the early years of the emergence of the Somali piracy phenomenon that risk was principally in the difficulty of getting on board vessels underway, some with high freeboard, at speed and generating a significant wake. At that time, when pirates were detained by the military fleets despatched to the Somali coast and the Indian Ocean, a policy of catch and release was applied (at least by some military, if not by all). In retrospect that policy seems bizarre.

Ultimately the Somali piracy threat spread right across to the west coast of India and into the Gulf of Hormuz, a 'choke point' for oil cargoes coming out from the Gulf, and therefore intolerable to both West and East. Attitudes hardened; naval vessels became more aggressive and commercial vessels were progressively armed (by state military personnel or private security companies (PSCs)); a small step back towards the nineteenth or even the eighteenth century, perhaps, an era softened only in fiction by temporal distance (*Kidnapped*, *Treasure Island*). At that time piracy (in the Caribbean) was suppressed with truly shocking violence; though looking further back this might be considered moderate compared to punishments gratuitously handed out on land under the Plantagenets and Tudors to impose a regime with an iron fist. Those found guilty of treason were hanged, drawn (eviscerated while still alive) and quartered (decapitated and the torso cut into four parts), a penalty originally devised for pirates in England in the thirteenth century. The regime for dealing with piracy remained exceptionally hard, under, for example, the Offences at Sea Act 1536 (under Henry VIII) and the Piracy Act 1698 (under William III). The death penalty for piracy was only finally revoked by the Piracy Act 1837 (under Victoria).

One of the last of the large, high-value, fully-laden blue water hulls ("SMYRNI") was taken in May 2012. I handled many such takings on behalf of ship owners, war underwriters and kidnap and ransom underwriters. Where else could one snatch what might be several hundred million dollars' worth of property and negotiate a ransom with relative impunity (and agree to release it in a settlement agreement and an informal verbal protocol of delivery)? The threat to blue water tonnage has abated because the physical risk to Somali pirates by the use of arms (navies, military personnel on board vessels and PSCs) began to outweigh the likely benefit (support for the argument that at some point some problems can only be solved with military strength?) It was also reduced by implementation of purely safety-oriented changes made on board by way of piracy preparedness and vessel hardening making boarding and holding ships more difficult (by the application of Best Management Practice (BMP)). These changes included razor wire, navigating at maximum speed and weaving, water cannons (monitors), the securing of doors with steel bars and the creation of 'citadels' (safe muster stations), the shipboard analogue of 'panic rooms'.

## Kidnap on land

Kidnappers have a similar method: capturing people and making threats to extort payment of ransom. Although another new phenomenon has emerged: virtual kidnapping (for example in Argentina, Mexico and Southern California), one new development in the proliferation of cyber risks and another step on the path to the 'no jobs' society? Physical kidnap presents some degree of risk to kidnappers where there is generally no safe haven to hold the detainees (in contrast to the waters just off the Somali coast); whether it is an 'express kidnapping' at an ATM in Mexico or Argentina or kidnapping and abduction to the Niger delta or into the threatening northern Nigerian provinces (the territory of Boko Haram, which also extends into Chad and Niger). This phenomenon, unlike piracy, is obviously not limited to the high seas or coastal waters.

In some places, kidnap is an ever-present threat on land. It may be done for ransom; it may be for other reasons (for example in Iraq, Syria and, previously, Lebanon); and there is nothing new about it. It may be as old as slavery (or, one is appalled to see, as new: 'UK family found guilty of enslaving homeless and disabled people', *The Guardian* 11 August 2017), or extortion or rape and pillage in time

of war or civil war. War and civil war can often reveal the thin line between civilised behaviour on the one hand and violence and degradation on the other, even in those who might otherwise be considered, fundamentally, decent men; to which the 'Terror' instigated by Robespierre in the French Revolution and the ugly spectre of les tricoteuses will attest (though there are many more modern examples). It does not seem to take much for society to descend into the world of *Lord of the Flies*.

Those land-based kidnap cases that I have handled have been in typical K&R hot spots (Mexico most notably, but also places that might be thought less obvious like India, neither of which could be described as a failed state). It is self-evident that K&R prospers in countries which experience, either in their geographic entirety or in their regions, some degree of lawlessness: Mexico, Argentina, Colombia, the Democratic Republic of Congo, Venezuela, Mozambique, the Philippines, Nigeria, Iraq, Algeria (at the Tigantourtine gas plant, for example), Syria, Yemen, Sudan, Pakistan (South Waziristan) and Libya. Or perhaps where there are unresolved racial, ethnic or religious tensions, such as for example along religious divides; hitherto the Balkans (now pacified) or at the dividing line between Islam in the north and Christianity in the south, right across West Africa and the Maghreb.

There may be an ever-present threat in such states, in some places. There is some observable overlap between risk of kidnap and states engaged in the modern war on illicit production and sale of 'recreational' drugs (Mexico and the Philippines, for example; the tide may have turned in Colombia). Paradoxically those states, which should be wealthy, potentially enormously wealthy, simply for the raw commodities that they can excavate for sale are not immune from the scourge: Nigeria (oil), Venezuela (oil) and the Democratic Republic of Congo (with its vast mineral wealth, notably in Katanga province). One might also think that those which have experienced economic collapse, for whatever reason, would also present risk; when money is tight, people fight. But this is not necessarily so. Italy in the 1970s would not have been described as a failed state, but nonetheless experienced a period of K&R activity, the kidnap and killing of the premier Aldo Moro in May 1978 being the most horrific example; and not forgetting the kidnap of Rolf Schild and his family, released for what was then a huge ransom in 1979. Nor indeed would West Germany have been described as a failed state, but it was nonetheless shocked by the kidnap and murder of Hanns-Martin Schleyer in 1977 by the Baader-Meinhoff Gang (the Red Army Faction). Nor moreover, looking back, would one have described the United States as a failed state. And yet this did not prevent the kidnap of the grandson of Paul Getty (the oil magnate) in 1973, or of Patty Hearst, the granddaughter of William Randolph Hearst (the press baron, son of the silver prospector George Hearst) in 1974; nor indeed looking back further to the kidnapping of the son of Frank Sinatra in 1963.

## Ransom or rescue?

The payment of ransom has been an effective means to secure the release of detainees from captivity for at least a thousand years, probably much longer. The enormous ransom paid to release Richard the Lionheart from the clutches of Leopold V, the Duke of Austria in 1192, is a case in point (hence 'a king's ransom'). Payment practically bankrupted the Privy Purse. Or for that matter the ransom paid to release Julius Cesar from the grasp of Cilician pirates (in 75 BC). More recently ransoms were paid by Frank Sinatra, by Paul Getty (after his grandson's ear had been cut off), by the family of Rolf Schild, and a large catalogue of ransoms were paid to Somali pirates estimated in some quarters at US$360 million or more (*Shipping Watch* 13 November 2013). Ransoms have been paid for the release of other land detainees. Indeed in contrast to the approach taken by the US and the UK, it is said that France, Germany, Spain and Italy have paid ransoms to release their citizens (*Independent*, 3 September 2013). It has obviously become far more difficult in the modern era to pay ransom when some governments have sought actively to discourage if not to proscribe the payment of any ransom whatsoever (whether to 'mere' criminals or to terrorists). Some simply ban the payment of ransom to terrorists; some ban ransom to recover people but not property. Whether ultimately this is a good thing for the detainees is another matter.

An alternative is to seek to recover detainees by force. It has mixed results and poses serious risks. The raid on Entebbe where hostages were taken for overtly political purposes (as with the capture of the "ACHILLE LAURO") is cited as a notable, indeed an extraordinary success, but many were killed or injured in the process. Two more recent examples come to mind where recovery was made without loss of life of detainees, "MAERSK ALABAMA" and the tanker "UNIVERSITY OF MOSCOW"; whether the pirates fared as well is a different matter. These were attacks on pirates during piratical attack, not after detainment was secured and the vessel sequestered off the Somali coast. They featured assaults by the US and Russian military. Other attempts at rescue by main force have unfortunately had a different outcome: the American doctor killed during a rescue assault in Afghanistan (September 2010), the Italian and British engineers, the latter executed to prevent rescue in Nigeria (March 2012) and the four American evangelists on a yacht off Somalia (February 2011). Ransom may be a distasteful concept, but it can save lives.

### Product tampering

Product tampering presents yet another opportunity or threat illicitly to extract cash, though, like extortion, piracy and kidnap, may also be perpetrated for political purposes, malice, corruption or greed (the China baby milk (melamine) scandal in 2008, the UK horse meat scandal in 2013). Those who might engage in product tampering for whatever motive also have a degree of physical risk. In some way they must contaminate or make product substitutions, which can only be done by physical intervention at some point; leaving a trail to follow, whether in DNA or otherwise.

Product tampering is one of the reasons that the manufacture of some of the most innocuous products, such as bottled water, toothpaste and tomato sauce, now requires screw caps and plastic and aluminium sealers; which would have been thought astonishing to those who were adults in the West in the 1960s or 1970s. The idea that someone would put something toxic into food products targeted indiscriminately on the general public is a distinctly modern phenomenon.

Even global brands must have some fear of product tampering or substitution, or the mere suggestion of it; indeed perhaps they have the most to fear since the quality and safety of their products – the very integrity of their brand - is the foundation of their fortune and their stock in trade (one reason, perhaps, why some of the world's most identifiable brands have social media war rooms, not only to manage attacks on their image). And all this is raises the spectre of the incurring of product liability by the manufacturer (which is beyond the scope of this paper).

In parallel, though for slightly different reasons, we live in a strange new era where innocuous items such as shaving cream and bottled water are plucked from the hands of aircraft passengers (tourists) before boarding flights, though not necessarily before catching crowded trains or boarding mass transit coaches travelling on crowded motorways. Even now such precautions are not applied to those entering underground stations (in London), notwithstanding the events of 7 July 2005.

One might seek to avoid or minimise exposure to the hazard of extortion, piracy, kidnap and ransom simply by avoiding dangerous places. And in the West at least, and no doubt elsewhere, the risk of exposure to product tampering may be small where the production and delivery chain is secure (from factory, to logistics companies, to wholesalers, to retailers, to customers); and where regulations (derided in some quarters) are devised, applied and policed, the very 'red tape' designed to provide safety and security (which find their analogue in BMP). This explains much of the ingenuity and curse of packaging, the crisis of waste disposal and the burden (and the genius) of recycling. It is not merely a matter of marketing and product vanity.

But it is obviously not always possible to avoid risk areas, by retreat into the gated estate. It will almost always be necessary to visit such locations or hot spots to conduct trade, to engage in mining and the extraction of raw materials; for example oil, gas, minerals (copper, iron ore, bauxite),

diamonds and precious stones. It may also be necessary to manufacture goods in low cost locations. And it may also be true for the mining of rare earths, 17 chemical elements to be found at the foot of the periodic table, primarily the lanthanide series, the names of which hardly trip off the tongue like the metals or the halogen gases. Mining for rare earths has become a pressing necessity because of the growth in health technology, the surge in battery technology (with the sudden rush of enthusiasm for electric cars) and most especially from the very boom in computers and communications which are the vehicles for the emergence and now the staggering proliferation of cyber risks.

But crime moves with the times. As we can see, the problem is clearly no longer limited to physical risk.

## 'New' electronic or cyber risks

Those who now engage in electronic piracy (by which I do not mean music theft) face different risks, as do those who are the subject of their unwanted attentions. And the potential victims cannot avoid these perils simply by staying at home, or by avoiding dangerous locations. These new interventions are not local, immediate and physical. This new generation of criminals (and juvenile rogues) can extend their metaphorical hands anywhere; across towns, cities, national boundaries, rivers, lakes and oceans, and into bank accounts and data banks, and now even to ships (and oil rigs?). Moreover, the perpetrators may consider that such electronic interventions expose them to less risk.

This may not be a perfect chronology, but, when the internet first started to spread and progressively PCs were put on all desks of those involved in any sort of administrative work at whatever degree of seniority, there started in parallel an illicit industry engaged in the creation of various sorts of trouble, whether merely annoying or deliberately damaging with a baffling new lexicon: malware, spyware, Trojans. Those creating the software on which the modern world is now utterly reliant, and without which it cannot function, have ever since been involved in a running battle to improve their products and to block access to the sensitive information loaded on them by the purchasers of their products. In a sense these are new ways to perpetrate old crimes, but may not be limited to that. There may be almost endless new ways to create mischief.

An overview with a little more detail of these sorts of problems would embrace the following hazards and threats within the broad category of 'cyberattack', or actions that can permit cyberattack:

- **Trojan/virus:** making the victim's computer run an unintended programme that will allow the attacker to gain access to private information, either by making the computer disclose this information itself, allowing the attacker direct access to secure information; or by allowing the monitoring of the use of the computer – for instance by the operation of a 'key logger' or other means of direct observation. In certain cases, the Trojan/virus may simply carry out predetermined damage with no further intervention from the attacker. Trojans are a device used to download ransomware.
- **Phishing:** aiming to confuse the victim into voluntarily disclosing private information, for example bank account details or the means of accessing other private information, such as how to access their Facebook or other social media accounts. Typically delivered in the form of supposed communications from the financial institution, internet service provider, or social media site, and almost impossible to distinguish from the real thing.
- **Monitoring of insecure networks and insecure communications:** collecting any passwords and any other un-encoded information, without the need to compromise any individual computer, only the network on which they are communicating.
- **Accessing known 'back doors':** provided for the convenience of the manufacturer, software author, or regulatory authority, bypassing the user's security.
- **Careless use of accounts:** some people are unwise enough to allow friends the use of their account details.

- **The wider release of data:** some service providers are hacked, by whatever means, and as a result release not only information that should be private to the users, but potentially also the means to further compromise the security of those users by gaining unsuspected access to their communications.

Attacks would target access to private information for the purposes of damage; some form of strategic advantage (commercial or political); and/or personal gain; or possibly simply mayhem and destruction, for example:

- Using the unapproved access, to attack others in turn (e.g. DDOS, using a massed array of 'zombie' devices, potentially in the future involving not only personal and other computers, but also smart home controllers, fridges, and potentially other white goods).
- Stealing passwords, to monitor private communications, to gain access to bank accounts and other secret information or to effect identity theft.
- Accessing compromising information (whether documents or photographs) that may have special value to either the target or some third party (including the general public) as a means of extracting cash whether by extortion or sale to some interested third party.
- Threatening damage to personal information or preventing the victim from accessing their computer (or computer systems of large users), for multiple purposes, and demanding ransom.
- Making threats even for the purpose only of impacting the victims' morale, or enhancing the morale of the attackers' friends and allies.

And all this might happen without the innocent user ever having taken the plunge into the fetid pool of the 'dark web', whatever that may be and however it might be found or accessed.

But people will inevitably want to continue to communicate electronically. One can see them in the streets heads bowed feverishly reading or tapping the keys, immersed in the virtual world. Alvin Toffler's dystopian vision (*Future Shock*) may have come to pass. So, perhaps unbreakable encryption will be the holy grail of the computer industry, following the development of the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) and subsequent developments, a form of modern Enigma machine? The Enigma machine, invented in Germany by Walter Scherbius after the First World War, was initially used for commercial purposes, though put to a different and more sinister purpose in the Second World War. The use of ciphers or codes must, after all, be as old human writing. Encryption might be exactly what is needed to protect users from theft perpetrated by electronic means.

But there are obvious countervailing pressures. On the one hand there is the obvious and natural desire of individuals for a private life, guaranteed for example by Article 8 of the Human Rights Convention (and Fourth Amendment to the American Constitution), and of businesses to communicate in private, not least in both cases to protect their financial affairs. But some states are increasingly troubled by the idea that they may not be able to gain access to information created or disseminated by individuals (vide: the views of the British Home Secretary, Amber Rudd: only terrorists (and criminals) benefit from encryption; 'real people' don't need it for WhatsApp (*The Daily Telegraph*, 1 August 2017), though some might beg to differ; and hence the running battle between Apple and the FBI to break encryption on iPhones (the so called Crypto Wars), *New York Times*, 21 March 2016, for example).

But how likely is it that unbreakable, inaccessible products or software systems will ever be devised as a means of protection against electronic threats, as opposed to physical threats? One can only guess; but in a world where teenage boys or young men can allegedly hack into the US Government's security systems (*The Daily Telegraph*, July 2016) or the computer systems at Cambridge University (*The Daily Telegraph*, April 2017) or into Microsoft (*The Daily Telegraph*, 25 April 2017) or allegedly even distort the US stock market (*The Daily Telegraph*, 22 April 2015, the so-called 'flash crash') one is

left to wonder. For example, *The Guardian* reported (in a Press Association article on 25 April 2017) that:

'Adam Mudd was 16 when he created the Titanium Stresser program, **which carried out more than 1.7m attacks** on websites including Minecraft, Xbox Live, Microsoft and TeamSpeak, a chat tool for gamers.

He earned the equivalent of more than £386,000 in US dollars and bitcoins **from selling the program to cybercriminals**' (emphasis supplied).

Theft and personal gain may not be the original motivation. But the consequences can still be devastating. The Press Association article on the Mudd case observed:

'Young people attack computer networks to impress friends and challenge political system, crime research shows. Mudd pleaded guilty and was sentenced at the Old Bailey. The judge, Michael Topolski QC, noted that Mudd came from a "perfectly respectable and caring family". He said the effect of Mudd's crimes had wreaked havoc "from Greenland to New Zealand, from Russia to Chile".'

All this is quite extraordinary (note again the involvement of Bitcoin). Whether the losses incurred are covered on policies of insurance is, however, a different matter.

We had previously lived in a world where knowledge was assimilated over years of study. The older generation had (generally) time to absorb vastly more information than youth and their actions were tempered by maturity, or at least by age. Youth, it was thought, recognised the wisdom of maturity, or at least was restrained by it. But it is now said that this no longer prevails ('Young revolutionaries reject the wisdom of maturity', *The Daily Telegraph*, 17 June 2017); and the 'certainties' that previously underpinned society have been overturned. In any event, the use of some modern software systems is simply beyond the comprehension of some of those in middle age and beyond, and who hold substantial resources. (Not that the new offences are confined to misguided youth.) The technophiles can be deeply troubling to the technophobes.

Matters which genuinely need to be kept secret for perfectly ethical business reasons, or as part of the dignity of private life or personal relationships, are now obviously at risk. One might be left with the axiom: it is a secret if you are the only one who knows (and store it only between your ears). But what is the use of a secret that is not and cannot be shared (an unpatented process, an idea, an intuition, an intellectual breakthrough?). Should we be reduced to writing down our best ideas in some obscure language, or refusing to publish them for decades (Newton), or writing in mirror writing or in codes (Da Vinci) with the risk that they may not be decrypted after death? Almost certainly not. There has been a huge surge in the desire to communicate, to disseminate information and to open up the arcane to observation and scrutiny. This is an irreversible change. It is dramatically easier to do so and perhaps as a consequence it is done with less care (see *Morphed in the Medium*, Clift, N.R, J D Supra, July 2010).

All this is part of a continuing trend, just as we have seen increasingly sophisticated attacks (though with a different purpose) in the maritime field (notably the drug traffickers' attack on the port of Antwerp in 2013, to get Colombian cocaine into Europe, *The Daily Telegraph,* 16 October, 2016) or the alleged attack in Sony Pictures in 2014 (*Huffington Post*, 1 September 2016). And only in the last few days have we seen what appears to be reporting of a credible threat to ship navigation in the shape of 'GPS spoofing' (*The New Scientist,* 10 August 2017).

Hence, again, it may be that significant emphasis needs to be put on robust systems to facilitate recovery after attack (since attacks cannot be wholly prevented) and getting insurance cover to mitigate the consequences, on terms, to the extent it may be available.

What about the penalties? Will ferocious threats of any type (in any jurisdiction) provide any sort of guarantee of deterrence? It remains to be seen. Just finding out that an attack has been made might be one thing, quite apart from measuring its consequences, still less finding out how it was done and ultimately who might have done it. When major businesses are unable to offer online services for a number of hours, for whatever reason, one is now simply left to ponder: is it another system failure, the cost of which can be and has been truly staggering, or something quite different? Is there an electronic equivalent of the tarred pirate corpse hanging in the gibbet (like the body of Captain Kidd, said to be Stephenson's original inspiration for *Treasure Island*)? Indeed, is cybercrime deterrence effective at all (See *Bank Info Security*, 1 June 2015)?

And setting aside rescue for the moment, when confronted by electronic extortion, piracy, ransomware or product attack what is the solution? How often has it been the case that the victims simply pay what is demanded as what appears to be the easiest and quickest way to restore normality, without realising perhaps the further problems that this might generate? There is a lesson in consequences here, going back to the payment of Danegeld, that people, companies and regimes have consistently failed to heed: once you submit to ransom, there is every likelihood your tormentor will come back for more.

In all this, the article in *The Times* on 5 September 2017 makes illuminating and troubling reading. This reports cyberattacks on British Universities targeting scientific, engineering and medical advances including research into missiles. A freedom of information request has revealed a doubling of such attacks in the last two years on institutions including Oxford University, Warwick University and University College London. The director of technology at Darktrace, a cyber security company created by mathematicians at Cambridge is quoted as saying that hackers are trying to get hold of cutting edge research in weaponry and energy. The head of cyber security at GCHQ's National Cyber Security Centre reports that Britain has experienced nearly 200 attacks in three months 'many of which threatened national security'. And a shadow Home Office minister is quoted as saying that underinvestment in [cyber] defence systems has 'left swathes of the public and private sector vulnerable.' This is certainly more than simply a matter of theft.

## Conclusion

This, then, is a glimpse at the new world of cyber risk, or some aspects of it, in comparison to old physical risks; a real hazard following the damp squib of Y2K. Cyber risk can now it seems be almost anything along a spectrum from the hacking of domestic appliances (your fridge?), the hacking of safety or security systems on cars, navigation systems on ships, all the way up to sophisticated attacks on state systems and, most particularly for the subject matter of this article, 'ransomware' such as the Petya attack in June this year and the WannaCry attack on the NHS and on companies as far afield as Spain, Russia, Ukraine and Taiwan the month before, and now the HBO attack.

The use of such devices or programmes presents new challenges and an ever growing need for teams of specialist personnel to handle attacks and their consequences; hence, in part, the proliferation of the whole new discipline of crisis management. This is why law firms have developed the equivalent of rapid response teams, in much the same way that maritime law firms have operated emergency hotlines for decades to respond to maritime casualties. These new teams are rather different, however, in that they must be able not only to commence urgent proceedings, seek freezing orders, seek search and seizure orders, but take urgent steps to sequester materials for electronic disclosure, exclude rogue employees from central systems and work closely with media advisors and a whole range of other experts, notably IT specialists. Computer science is no longer the dull field of the blank screen and the flashing white cursor.

It has not been necessary that we should be visited from some post-apocalyptic world to be threatened by our own machines. Nor do we need to be worried that they 'will be back'. They are already here. And now, when one is looking at the screen and keyboard each morning on starting work (or compiling a simple order to purchase groceries) one is left to wonder: who is watching, who is looking back through the laptop camera or monitoring and collecting the keystrokes? Is it merely a dumb terminal? It may not be what Orwell meant or intended, but perhaps we are indeed now observed by Big Brother. Sophisticated users (it is said) put tape over the cameras of their phones and computers, which they remove only when these are specifically needed for their own use.

No wonder, then, that there is currently pressure to establish a 'right to be forgotten', to slip back into privacy and invisibility; and the drive to implement the General Data Protection Regulation (Regulation (EU) 2016/679), to be in force by 25 May 2018. Do we stand within the stable listening to the clatter of the departing hooves as the door swings reprovingly on its hinges?

And, if it is tempting to say we can solve many if not all such hazards and difficulties by getting better (cyber) security, the inevitable response must be 'quis custodiet ipsos custodies?' ('Who will watch the watchmen')?

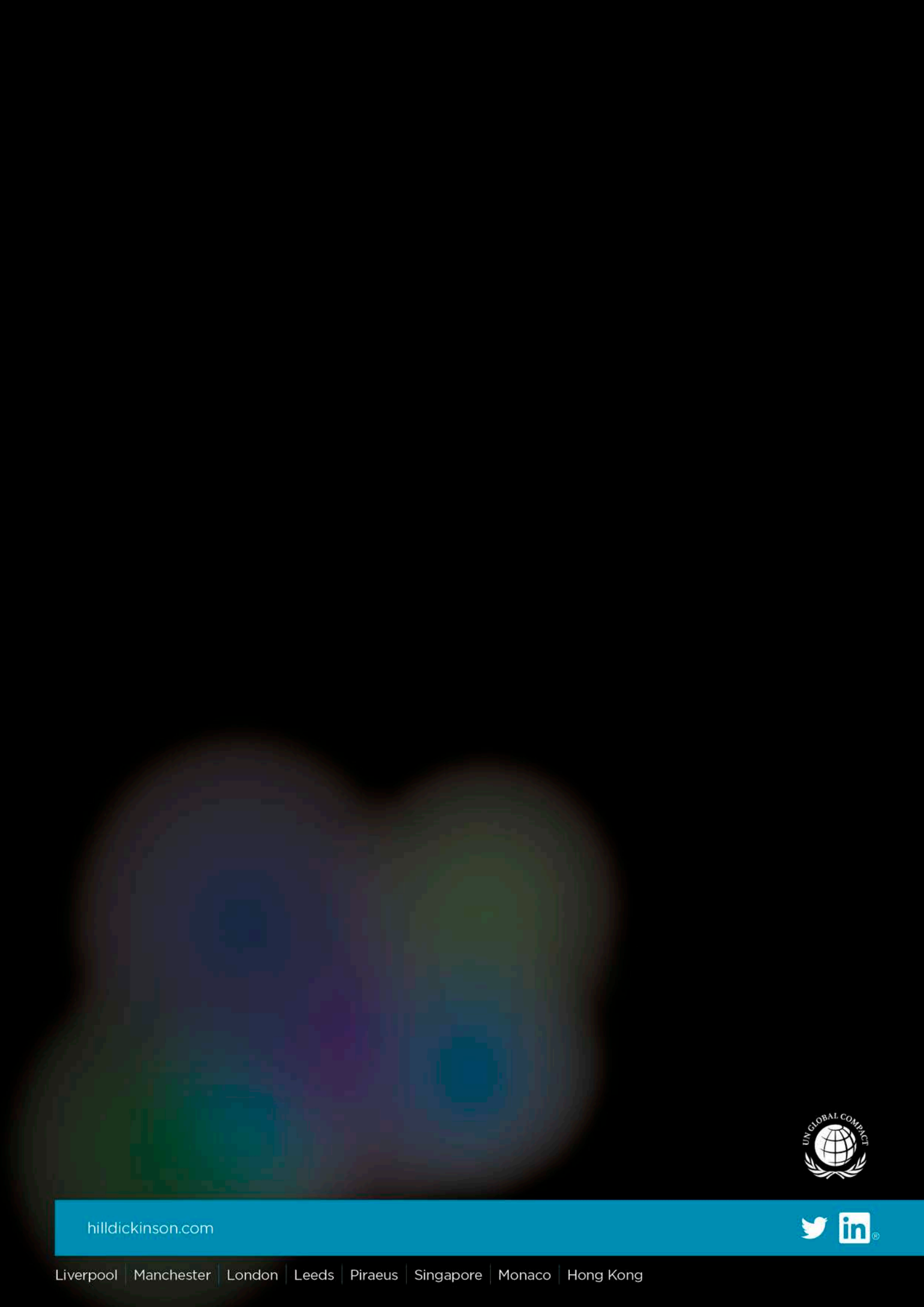
Systems and regulation are likely, nonetheless, to be a significant part of a developing strategy to contain these emergent problems. As to the maritime world we have The Guidelines on Cyber Security Onboard Ships, the second edition of which was published on 5 July 2017, compiled and endorsed by a number of industry bodies: BIMCO, INTERTANKO, INTERCARGO, CLIA, ICSKO, OCIMF and IUMI, with input from multiple participants in the maritime sector, and in that sense similar to BMP and with similar objectives. Such guidelines are likely to evolve as the problems evolve and proliferate. They, and their equivalents in other fields, may have to evolve very rapidly indeed.

Perhaps cyber hazard or cyber risk will penetrate or already have penetrated, in some hidden, anonymous, nebulous shape or form, almost every aspect of our personal and professional lives, every facet of public and private life; of our industries, factories, hospitals, financial institutions, educational establishments, and all means of transport (cars, motorbikes, ships, trains and planes, whether manual, remote controlled or autonomous) just as computerisation and IT systems are now simply ubiquitous: a sobering thought, and a reminder to us to take greater care.

This, then, is our brave new world.

Rhys Clift


rhys.clift@hilldickinson.com



hilldickinson.com

Liverpool | Manchester | London | Leeds | Piraeus | Singapore | Monaco | Hong Kong