Standards Today

A Journal of News, Ideas and Analysis

A publication of CONSORTIUM INFO.ORG GesmerUpdegrove LLP

July 2013 Vol. XI, No. 1

CONSIDER THIS:

#68 The Devil's in the Cloud: It's Time to Stop our Headlong Rush into Cyber Insecurity

Andrew Updegrove

There appears to be consensus in many quarters that migrating to the Cloud is highly desirable – indeed, that mass migration is already inevitable now that the technology as well as the bandwidth finally exists to make remote hosting viable.

And why not? Multinational IT vendors view this transition as the next great market opportunity; governments see in it a chance at long last to rationalize their Byzantine legacy systems without incurring massive up front capital costs; and enterprise users find the value proposition increasingly compelling as their locally-based systems become more complex, expensive and difficult to maintain.

Meanwhile, an ever increasing torrent of data, records, photos and social relations of everyday individuals leap with the tap of a key from hard drives and back up devices under the control of their owners to servers located who knows where, owned by who knows who, and vulnerable to who knows what?

As this process continues, all-too predictable market forces will drive cloud services towards commoditization, and with commoditization will come consolidation – again, in response to classic market dynamics.

As the share of global electric power consumed by data farms and networks approaches an incredible 10%, concerns over climate change and rising energy prices continues to drive the data farms that receive all this data to cluster around the lowest-cost energy sources – wind farms, hydroelectric dams and, someday, perhaps solar and geothermal sources as well. Already there are millions of servers humming in data farms adjacent (for example) to the Columbia River in Washington state that dwarf the agricultural farms that they have replaced.

Ten years from now, what percentage of all that matters will be hosted by an increasingly smaller number of ever more enormous data complexes? Not just the transactional wherewithal to enable transportation, finance, government, food production, power transmission, manufacturing and education to function, but – far more consequentially – what percentage of all data: technical, financial, civic, cultural, commercial, indeed, all human knowledge? No longer will any of this data be archived in non-electronic form (i.e., on paper). It will, of course, be backed up electronically – to other data farms.

Let us add one final trend: as the First World becomes more networked and Cloud dependent, its asymmetric vulnerability to less network-reliant enemies will increase exponentially. After all, when the United States has a military budget equal to that of the next 17 most militarily committed nations combined, what incentive can there be for a lesser country that wishes to tweak the lion's tail to spend a Rial or a Won on traditional weaponry?

This last trend has been well-recognized as a reason to take electronic cyber security seriously. But this realization masks a far more serious vulnerability entirely, because systems that are the victim of a cyberattack can usually be restored again – often within hours. But the data hosted at a facility that has been transformed into a smoking ruin by kinetic weapons of war or a terrorist attack will never be brought back on line again if its back up site is in ashes as well.

As we will explore below, in a cloud-based world, it will be remarkably simple for any nation – indeed for the entire First World – to be reduced to a state of societal collapse by an enemy whose identity may never be learned, much less determined while the nation is still capable of retaliating.

The moral of the story is that equal attention will need to be paid to developing and mandating adherence to standards ensuring physical as well as electronic security for our increasingly Internet-dependent modern society. To do otherwise will be to render ourselves vulnerable to a degree of societal destruction that would rival that produced by a nuclear war, and which will soon be within the technical capabilities of dozens of nations throughout the world.

Ten years from now, what percentage of all that matters will be hosted by an increasingly smaller number of ever more enormous data complexes?

Does that sound improbable and alarmist? Let me suggest that you consider the following scenario before drawing a conclusion.

New Year's Day, 2023

As the sun set on New Year's Eve, 2022, a dozen anonymous container ships are decreasing speed a few miles outside major American and European ports. Like many carriers nearing the end of their useful lives, their histories are mongrel in nature; some had been commissioned by shipping magnates in Greece, while others had been ordered from points around the world. Each had passed through multiple hands and now sailed under Panamanian registry or one of the other common flags of convenience; and each had been chartered three years ago by one of an equal number of shell companies formed in third world countries scattered around the globe.

The terms of each contract made the charter party responsible for the upkeep of the ship it had leased, and therefore in due course each ship had undergone repairs in small ship yards in the Indian Ocean and in Southeast Asia before returning to ply its trade in the various shipping lanes of the world.

Over the two years that followed, the ships loaded and unloaded tens of thousands of anonymous containers. As one might expect, they contained almost anything a container could hold – phonebooks from printers in Calcutta destined for telecommunications carriers in France; timber transshipped at the mouth of the Amazon consigned to furniture companies in South Carolina; consumer electronics from Taiwan bound for Southampton; plywood shipped from Kyoto to Seattle made from trees that had been cut in Oregon and shipped from Portland to Kyoto only a few months before. All of the infinitely varied stuff of global commerce that passes from point A to point B before being transferred to trucks and trains for forwarding to points C and D.

Frequently, the ships traded cargoes in ports in Africa, India, Indonesia, Bangladesh and other parts of the Indian Ocean and South Pacific.

There was therefore nothing to remark upon as the members of the aging fleet neared their current destinations: some were closing on Seattle, Los Angeles, New Orleans, Newport News and Boston. One had steamed up the St. Laurence Seaway, through the lakes and locks and onto the broad waters of Lake Michigan. Others were nearing ports in the English Channel, the Baltic, and the Mediterranean. The papers of each ship were in order, and a pilot was already scheduled to guide each to the dock that had been reserved to accept its cargo.

To the practiced eyes of the pilots, each ship would be different, although all were of approximately the same tonnage and design. But any pilot would swiftly note two aspects of each ship that would stand out. The first was that its hull had been modified to install large doors in its stern, ostensibly to allow roll on/roll off handling of cargo. That would be curious, because each ship had also been configured to carry containers, which would most often be loaded from above.

The only indication that something unusual was afoot was the low hum of the propeller-driven drones – hundreds of drones

They might also wonder what port each ship visited that was configured to load from the bow, rather than from the side. But with 70,000 commercial vessels plying the seas, they would have seen almost everything before.

The second aspect was that each ship was riding unusually high, showing more bottom paint and Plimsol lines then one would assume for a ship carrying a profitable cargo of tightly packed containers.

In the dark of the night, though, none of these peculiarities would be visible. Nor was anyone near enough to notice as the doors in the sterns of the ships swung open, because all lights had been extinguished inside. The only indication that something unusual was afoot was the low hum of the propeller-driven drones – hundreds of drones with muffled engines – emerging in rapid succession from each ship before pursuing its unerring course towards its target. They flew only a few hundred feet above the water, and then over the land.

Some of those targets were only a few score miles away, while others were many times more distant. It hardly mattered, though, because the United States and Europe had been secure within their borders for many decades. In the modern world, only the United States, with its ten carrier fleets, could project real military muscle against distant enemies. Why, then, would any First World nation need the types of coastal anti-aircraft defenses they had constructed before the advent of the nuclear age? These fortifications had long ago been abandoned and fallen into ruin.

Needless to say, confusion reigned as the first drones began striking their targets. The small night time staffs working at the targets had no way of knowing what was hitting them –

Truck bombs crashing through the chain link fences that surrounded the installations? Missiles? And from where?

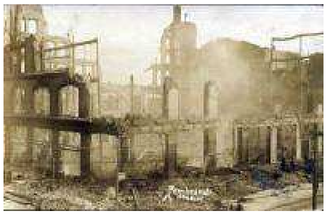
Only after the destruction was complete did the realization spread that the nations were under a coordinated attack. Their governments and militaries struggled to understand what had happened, and to react. But the drones had all been destroyed, leaving few clues. And still under cover of darkness, the ships that had launched the attacks had sunk quietly beneath the waves as their crews raced out to sea in speedboats, there to be taken aboard by other ships that had left the same ports the night before. These vessels were equally anonymous, except for the hoists that allowed them to swing up the speedboats without deviating from their courses or decreasing their speed, and then to lower them in a matter of minutes through the open hatches that rapidly closed once more.

The countries that had been struck launched no counterattacks, because there was no way to know who to attack without weeks of investigative work. Even after the identity of some of the scuttled ships was established, it was laborious to work through the tangle of seemingly endless layers of holding companies controlling them. And the drones could have been loaded in any of the hundreds of ports the ships had visited over the preceding years.

The civil and military leaders of the target countries never did completely understand what had hit them. To do so would require sophisticated networks to gather and analyze data of all kinds.

And that was now impossible. Because, of course, the targets the drones had destroyed were the data farms.

The New Dark Ages



When the New Year's Day sun rose in Europe and the United States, the reality of what had happened was hidden to almost all. Only a hundred or so targets had been struck, and the smoke from the devastated facilities was already dissipating. What people did realize immediately was that a great many things that they were used to working now did not.

What no longer functioned included anything that relied on electricity or the Internet. Which was, of course, virtually everything except automobiles and hand tools. This was necessarily the case, because all of the elements that coordinated and controlled the power grid had been destroyed. Even many battery powered devices were silent – the cell phones had no dial tones, and the radios generated only static, because the management software and servers that enabled telecommunications had also been annihilated. Perhaps most discomfiting of all, there was no Internet, nor any of the services that relied upon the Internet.

For the first few hours, the effect was unusually peaceful, the way a power outage can sometimes be. Neighbors in the Deep South of the U.S. remarked upon how nice it was to simply sit on the porch and talk, just like the old days.

But by mid-day, the novelty was replaced with consternation, because there was virtually no information available about what had happened, and how it would be made right. True, some emergency broadcast radio channels were operating, but because the authorities that controlled them had so little knowledge about what had happened, or the extent of the damage, there was little they could say. Worse, if they had shared what information they did have – that those ostensibly in control had no idea how they would go about restoring the power grid, let alone the Internet, in any reasonable amount of time – mass panic would certainly ensue.

There was little to prevent the arrival of that state of affairs in any event. For those that were fortunate, it was a matter of days. For others, it arrived before the night of the first day had fallen. Riots and looting broke out in many cities, fueled in part by fear and in part by opportunism.

By the second day, the true severity of the situation began to penetrate the consciousness of more and more people. The gas in the tanks of their cars was the last gas they would have until who knew when, because gas stations had no generators. Even if they had, there would be no more deliveries of new fuel to the stations, because there was no more Internet to support inventory and shipping controls to monitor supply or demand, or to restart the refineries, all of which had immediately shut down and could no longer be controlled.

Needless to say, the banks did not open. Nor did ATMs operate, although in truth the relevance of paper money was rapidly becoming less and less obvious. The capital markets stayed closed as well, as did almost every element of the transportation system, dependent as they were on computerized management, and as workers became less and less willing to use precious gasoline driving to work.

As the fuel ran out in cars and trucks, the delivery of even locally available essential items – food, heating oil, medicines, clothing, replacement parts – speedily came to an end.

As had always been the case in the past when a natural or man-made disaster had struck, police, firemen, EMTs and other first responders sprang into action. But this time, everything was different. For one thing, they lacked reliable communications. For another, they lacked information.

What no longer functioned included anything that relied on electricity or the Internet. Which was, of course, virtually everything

Databases that used to live on local servers had long ago been moved to the distant data farms. Information as basic as the addresses and phone numbers of a police department's own personnel was suddenly unavailable. Desk sergeants were reduced to rummaging through desk drawers, hoping that someone had printed out a copy of one piece of information or another for temporary reference.

The same crisis developed quickly in almost every other setting. Hospitals relied on power from backup generators, but only for a few days until their fuel supplies gave out. Their patients no long had a medical history to consult, because paper records had all been replaced with electronic medical records. All of those records – of course – were remotely hosted, or at least had been, prior to the attack. Now they had ceased to exist. Nor could doctors order medical tests, because the servers that hosted the diagnostic software also no longer existed. Only the oldest doctors had ever been trained to diagnose through personal observation. The younger ones found that suddenly they were scarcely more competent to treat their patients than were the patients themselves.

So also at airports, where suddenly air traffic controllers and pilots were reduced to line of sight, visual navigation; pilots with rapidly emptying fuel tanks circled nervously over airports waiting for clearance to land. Once down, they did not take off again, because every airline shut down its operations; they had no way to know who had paid for a ticket who had not, or whether planes would be full or empty, or whether there would be sufficient fuel at any given airport to refuel a plane once it had arrived.

Buses, of course, needed fuel. And soon they had none. Railways were only a little better off, because their signaling systems no longer functioned. That hardly mattered, though, because the local lines and spurs that long ago carried rail freight from main lines to factories and small towns had long ago been abandoned. There was little point to moving items from one transshipment point to another, since there were no longer any trucks to complete the delivery to its final destination.

First responders did the best they could at the local level for as long as they could. But as time went on, what they could do became less and less. They had no food to dole out, nor any way to bring heat to the emergency shelters that had always served their appointed purposes in the past. As the reality of the situation began to sink in, police, firemen and ambulance staff did what could be expected – without fuel to commute, they returned to their families, to do what they could to protect them instead.

Meanwhile, supplies of medications at pharmacies and hospitals rapidly dwindled. When stocks of insulin and other urgently needed medications gave out, the results were both predictable and tragic.

The shock of realizing that vital information had been lost – perhaps forever - played out over and over in millions of businesses, universities and government agencies in the days that followed. The impact was numbing and immobilizing. Theoretically, over many months millions of new servers could be ordered, built, bought, shipped and installed, and those servers could theoretically be reloaded with software and that software could be reconfigured, over another very long time. But how could those servers be manufactured, much less ordered, paid for, shipped and installed without access to the data, software and computing power that had been destroyed? Over time, perhaps, yes, but how to accomplish anything at all until that had occurred? Or survive until it had?

So it was with the power grid as well. The days were long gone when every town had its own generation facility. Instead, the grid had become like an ocean of power into which producers poured electricity and from which users pumped it out, matching up accounts between buyers and sellers through highly complex software. Maintaining that grid had become an almost infinitely complex balancing act. Take down one part, and the impact could cascade through a wider and wider area. Bringing it back up was a vastly intricate job, predicated on the assumption that virtually all generating capacity would be available to once more be linked together.

True, wind turbines continued to turn and the dynamos deep inside hydroelectric dams still spun. But renewable energy constituted only a very minor part of total energy needs, and little of that could now be distributed. The coal-powered facilities that remained continued to produce, but only for a few days, until their on-site coal supplies ran out, because the transportation system was down. Gas-fired plants had already shut down when the pipeline system crashed, due to loss of the systems that controlled distribution. Naturally, all of the nuclear facilities were shut down immediately, out of fear that they could be the next targets of attack.

Every way that those in charge sought to turn, there were missing pieces – missing pieces in everything and everywhere. It was as if in an instant all of the modern infrastructure of two continents had been turned into confetti and blown to the four corners of the earth. Here there was still a bit and over there another, but too much of what should have been in between was unavailable to allow anyone to start to repair anything at all. And really, there was no place to start, because your communications were down, as your analytical tools were no longer available.

In the best of times, perhaps it could all have been put back together again. But these times were anything but fortuitous. To rebuild would require vast amounts of coordination and communication. But chaos increasingly prevailed in the streets as food and fuel ran out. Soon, only the armored vehicles of SWAT teams and the National Guard could safely move about, when they had the fuel to do so. Those charged with maintaining order and with restoring normalcy became first, demoralized, and then desperate. Finally, they became powerless, and mass desertion set in. Who could blame them?

It was both cruel and deliberate that the attack had been unleashed in midwinter. Those who relied on natural gas for heat were immediately at risk of freezing to death, while those relying on oil were able to keep the cold at bay only until their tanks ran dry – assuming they could run without electricity. Those that had full tanks stayed warm while they starved; it did not take long to consume their last canned goods. That is, if they had not been stolen by their neighbors first.

Except for isolated pockets of elected leaders sheltering at military bases that could do little but preserve their own safety, all federal, state and local governments had utterly collapsed. Soon, well-armed, but hardly well-ordered, militias began to spring up. In most cases, they brought more fear than safety to the territories they staked out. Incredible as it would have seemed only a few months before, much of the first world was under the control of what could only be called war lords.

It seemed incredible that the often imagined cinematic scenario of a dystopian, post-apocalyptic nightmare world had been made real so easily, and in such faithful detail. Not by means of thousands of nuclear weapons delivered by intercontinental ballistic missiles, but by squadrons of simple, but well-targeted drones bearing conventional weapons, launched from a tiny fleet of out of date cargo ships.

In the face of such enormous need, the rest of the world did what it could, which was not very much. A few nations sent relief efforts to coastal cities, but many of those efforts were met in the United States by armed mobs intent on getting as much as possible for their starving families. Soon, these efforts ceased. And indeed, with more than 800 million people in Europe and the United States in the worst need imaginable, and with no means to distribute what they so urgently required once it had arrived, what could a poor or a small nation do to make a dent, in any event?

And then, of course, there was the danger that whoever had attacked the West could also attack anyone that came to its aid.

By the time that spring had arrived, most of the population of northern Europe and the Northern United States had starved to death, been killed, or (in some cases) killed themselves. Many of those that lived farther south were not much better off. There were few seeds to plant where they were needed and there was no fuel for the tractors. They could hope to hold out until what few crops they could plant and hoe by hand had matured.

The Ghost of (Cyber) Future

It would be convenient and consoling to pretend that what I've just described is simple science fiction. But sad to say, the only thing that is doubtful about the scenario I have described is that it might be difficult for a perpetrator to build a thousand drones without Western espionage becoming aware of the plan.

But would that really be so hard? Many countries are building drones now; the technology is not complex. Indeed, Germany successfully launched V-1 drones against Britain more than seventy years ago, and they were jet powered. With the availability of GPS-guided navigation today, building and guiding sufficiently reliable drones of the primitive type needed to stage the type of surprise attack I have described is not only within the technical ability of every nation that could be imagined to be a suitably disposed enemy today, many more besides. And there are plenty of old ships to go around.

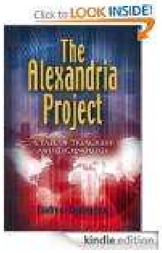
The moral of the story is that we are rapidly and willingly creating a vulnerability of astonishing severity, largely sacrificing the difference between our $650 billion annual military budget and that of a third world nation.

And I use the word 'rapidly' advisedly. There is already an Office of Management and Budget (OMB) program in place called the Federal Data Center Consolidation Initiative (FDCCI), under which the Federal agencies are closing 1,200 out of about 2,900 data centers. But this may only be a first step. The Department of Homeland Security has already consolidated its information much more drastically. Where once its enormous data resources were spread across 46 data centers, everything now is hosted by *just five*. As noted in a recent FCW.com article, "although having fewer data centers gives would-be attackers a smaller zone to target, the threat is offset by a smaller perimeter that has more controlled resources within it."

That may be fine if you are only worried about terrorist attacks by a few individuals. But it also dramatically increases the damage that a successful attack could do if some or all of those centers are breached. And it's abundantly clear that unless those five centers are buried deep underground, the type of scenario I've described could already have devastating effect today.

So why are we doing this?

In part, it is because it is easier and cheaper to place servers in lightweight industrial buildings. But the more honest explanation is that we live under the illusion that because we have not had a major war on Western soil since the 1940s that it cannot ever happen again. Which is, regrettably, patently absurd. Indeed, war has been intermittent in the Middle East for decades, periodically threatening to spill beyond those borders. Only two decades ago, a murderous and savage war was waged in the Balkans. How much more likely would an attack become if a drone-filled ship could replace an army, navy and air force all rolled into one, and without incurring a single casualty on the attacker’s part?



One need not look to the indefinite future to find a reason for concern. On what evidence should we assume that North Korea or Iran would never try such a gambit, and especially if it were possible that we would be unable to trace the attack to its source in time to retaliate? Even if we assume that currently known adversaries are not to be of concern, what about ten or twenty years from now, as the global population expands, and as water and other natural resources become ever scarcer?

If the picture I have painted is dreadful to comprehend, it should be. If we continue on our current course of centralizing Cloud services without housing them in appropriately protected environments, we cannot assume that a scenario such as the one described will certainly occur to one or more nations in the foreseeable future. With 5,000 years of war-torn history to look to for precedent, we would be reckless to assume otherwise.Happily, and unlike the challenges presented by cyber attacks, addressing the threat described is not even difficult. Only expensive, although not prohibitively so. The most obvious solution is simply to mandate that critical ((broadly, and not narrowly defined) Cloud services and related infrastructure, as well as critical data be hosted underground. Indeed, the medieval solution (fortification) remains beautifully suited to the current, modern risk. There is nothing technically challenging about digging a hole in the ground, filling it with a data farm, and covering it up again with 30 feet of dirt and reinforced concrete. It's only a matter of committing to incur the extra cost (if you're wondering what such a structure would be like, I've described one here).

While it's true that the U.S. today has a "bunker busting" bomb capable of reaching deeply buried resources, the U.S. is the only nation that has a stealth bomber capable of carrying such a 30,000 pound behemoth. It is difficult to imagine how any nation could successfully mount a concerted attack against U.S. data centers using ordinance of this nature for the foreseeable future. And unlike the drone scenario, existing defenses exist to detect and defeat such an attack, as well as to immediately determine its point of origin.

What is needed is for a thoughtful set of requirements to be set out that identifies data and critical infrastructure, and then specifies what level of protection against kinetic attack will be required to defend it. Happily, the identification of such infrastructure is already in process in the U.S. under an initiative launched by the Obama administration. Less happily, many areas of commerce are scrambling to avoid falling within the definition of "critical infrastructure" in order to avoid to the costs of complying with regulations relating just to thwarting cyber attacks.

As stark as the scenario described may be, it's hardly surprising that we should find ourselves at such a pass. Realizing the promise of the Cloud has been just over the horizon for twenty years, and now, suddenly, it has come within our grasp. Moreover, technical opportunity has always beguiled us; increasingly, our society wants to enjoy the candy first, and worry about the cavities later. Stated another way, profit motives will always bring innovation to the marketplace faster than prudent rules will be devised to protect us from any undesired but nonetheless real dangers that might come along for the ride. Even when real danger becomes too obvious to ignore, lobbyists weigh in to fight new restrictions and costs, and legislators temporize and delay. Sadly, the longer we delay requiring physical protection of data farms, the greater the resistance will be, because of the investment already made in unprotected infrastructure.

What we need to ask ourselves, like Scrooge in the Dickens tale, is which future do we want to live in? History tells us clearly that we have not seen the last of war. Europe especially should resonate to the possibility of a kinetic attack.

But those in the United States should pay even greater heed, because after centuries of living safely behind our oceanic moat, we now live in an age where a handful of aging ships can truly bomb us back into the Stone Age. The time to protect ourselves from such a risk is now.

Read more *Consider This*... entries at: http://www.consortiuminfo.org/blog/

Sign up for a free subscription to ***Standards Today*** at

http://www.consortiuminfo.org/subscribe/2.php?addentry=1