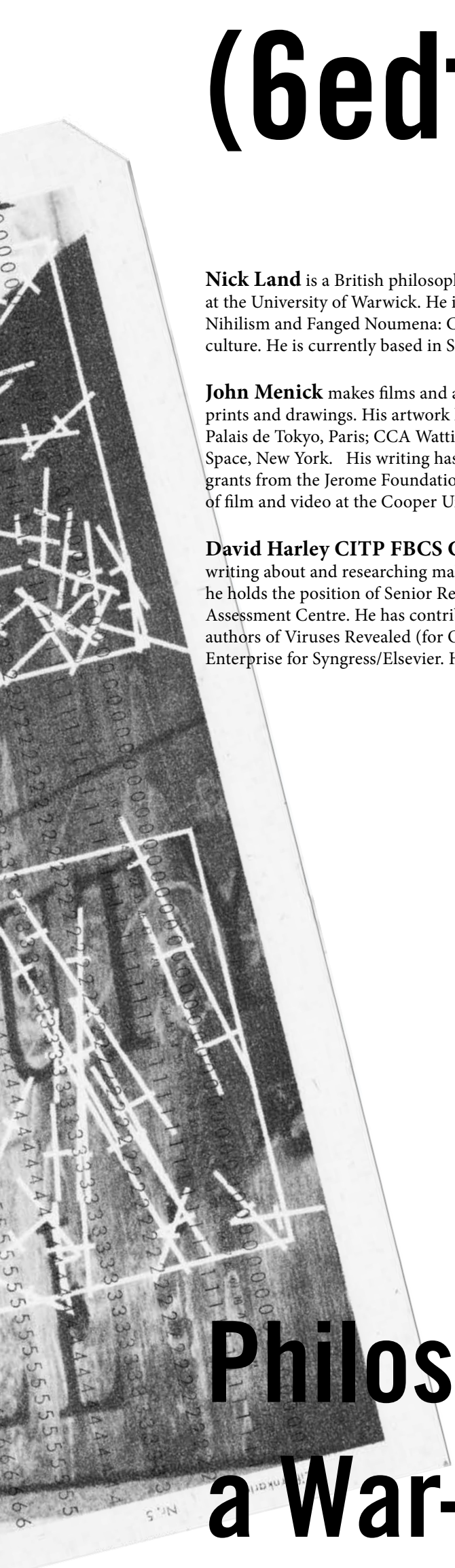
Dissolution (6edfsdf4c7e7)



Nick Land is a British philosopher and was a lecturer in Continental Philosophy from 1987 to 1999 at the University of Warwick. He is the author of The Thirst for Annihilation: Georges Bataille and Virulent Nihilism and Fanged Noumena: Collected Writings 1987-2007, along with various articles on cybernetic culture. He is currently based in Shanghai and runs the blog xenosystems (http://www.xenosystems.net/).

John Menick makes films and audio works, writes essays and short stories, and occasionally makes prints and drawings. His artwork has been shown at dOCUMENTA (13), Kassel; MoMA PS1, New York; Palais de Tokyo, Paris; CCA Wattis, San Francisco; Midway Contemporary Art, Minneapolis; and Artists Space, New York. His writing has appeared in Frieze, Mousse, and Art in America. Menick has received grants from the Jerome Foundation and the New York Foundation for the Arts, and he is a visiting professor of film and video at the Cooper Union in New York.

David Harley CITP FBCS CISSP is an independent researcher and consultant who has been writing about and researching malware and security since 1989. He has been working with ESET, where he holds the position of Senior Research Fellow, since 2006. Before that he managed the UK NHS's Threat Assessment Centre. He has contributed chapters to over a dozen security books, and was one of the primary authors of Viruses Revealed (for Osborne/McGraw-Hill) and The AVIEN Malware Defense Guide for the Enterprise for Syngress/Elsevier. He is a Fellow of the BCS Institute (formerly the British Computing Society).

Compiled by:

Lars T C F Holdhus
www.larsholdhus.com

Graphic design by:

Michel Keppel
http://michelkeppel.nl/

Philosophy in a War-Zone

Nick Land

"War is deception" – Sunzi

"War is the father of all things" -- Heraclitus

"War is god" -- Cormac McCarthy (Blood Meridian)

"You have made your way from the worm to man, and much within you is still worm." – Nietzsche (Thus Spake Zarathustra)

Camouflage

In a reality at war, things hide. The alternative is to become a target, a casualty, and thus – in the course of events – to cease to be. When war reigns, ontology and occultation converge. The oldest of all alliances binds survival to the shadows.

Absent a sovereign peace, of the kind an all-powerful and benevolent God -- or its political proxy -- could ensure, existence is a jungle of lies. Within such an environment truth, or unconcealment (ἀλήθεια), is a way to get things killed.

To see is to eliminate, actually or virtually, and with virtual elimination comes dominion. This is to return to pacific sovereignty on a darker (but illuminated) path. If no God is found already at work, announced unambiguously through a manifest peace, then a substitute has to be made from the suspension of war -- and that presupposes a war. A God who hides blesses only battlefields, because his stand-in will be a state.

In a war there can be no philosophical innocence (and there has never been philosophical innocence). Even when epistemology pretends to concern itself with things that we just happen not to know, its objects infect it with dissimulation, camouflage and secrecy, making it complicit in the transmission of the lie. It plays out war games of concealment and exposure, disinformation, distraction, and feint, entangled in the complex skein of signal manipulation and evaluation known to all militaries as 'intelligence'.

To know, or not to know – these matters are too important to be ignored by the war. It is through such discrimination that the difference between life and death is decided, and distributed. This is how the administrators of war, at their most confidently articulate, speak:

There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know. Who are we? ('We' don't know …)

Escalation

Before beginning over, from the end, there are some things to be said about ends. What modernity finds thinkable in war is owed, above all, to Carl von Clausewitz, and his great synthesis of organized bellicosity with rational statecraft, under the principle that *war is politics by other means*[1]. Politics supplies the end, and thus the war aim, to which all strategy and tactics is subordinated, in accordance with a rigorous teleological scheme. Military purposes have their final cause in the rational self-interest of the state.

Within the Clausewitzean philosophical system, the military apparatus is essentially technological. The entirety of its social and technical composition is comprehensible as teleological machinery, integrated in accordance with a command-control hierarchy of cascading purposes, connected to a transcendent political will. From the boots and bullets that constitute its simplest pieces of equipment, through tactical drills and maneuvers, to large scale strategic plans and operations, it can always meaningfully be asked: What is this for? Furthermore, this question is necessarily strictly equivalent to asking: How does this serve the ultimate war aim? War in-itself, however, is an emergent phenomenon, arising between states – rather than in subordination to them – and thus eluding the political meaning that corresponds to finalistic intelligibility. A war, *as such*, is not *for* anything (not even 'for oil'), unless it is misleadingly identified with the highest level strategy of one or other antagonist. Within the war no less than two ultimate aims, or political wills, collide, so that -- of necessity -- it can have no unambiguous purpose. Consequently, we cannot ask: Who is the war? Or: *What does it want?* (That would, or course, be insane.)

Nevertheless, Clausewitzean war has an inherent gradient, which simulates purpose to an arbitrary level of approximation. In accordance with its own nature, to which the antagonistic agents are pressed into compliance, war tends to *an extreme*. In other words, any restricted form of warfare is conceived as fragile political artifice, stubbornly subverted by a trend to escalation that expresses the nature of war in-itself, and which thus counts – within any specific war -- as the primary axis of *real discovery*. A crypto-teleology proper to war itself is demonstrated by the inclination of violent, politically-uncircumscribed conflict to escape all limitation.

From the perspective of the state and its serious games – which, as we shall see, can be transferred beyond the state onto trans-political confrontations of an even more radical nature – it is not difficult to understand how escalation (*the autonomization* of war) takes over. Insofar as the state approaches its historical essence, as a sovereign or ultimate entity, military defeat is a catastrophe that cannot in principle be transcended. From the intrinsic character of the state, it follows that *no measure required to avoid defeat can be excessive*. The epoch of nuclear confrontation, which – contrary to superficial appearance – has scarcely begun, has facilitated the rigorous formalization of this macro-political incentive to the abandonment of limitation, all the way to Mutually Assured Destruction.

Conceived concretely as a relationship between antagonists, rather than abstractly as a gradient of war in-itself, escalation is a zig-zag of reciprocal incitement, or a cybernetic circuit without negative (dampening) links. The structural predisposition of each party to escalation is carried forwards, or advanced in time, as an efficient virtuality, reinforcing the positive trend with a supplementary motive for pre-emption. The probability that the enemy will at some point escalate becomes a prompt for anticipatory counter-escalation, creating a wave of intensified war effort with reversed time signature. The model war is maximally-accelerated escalation provoked by the future: Time pressure.

Threat Matrix

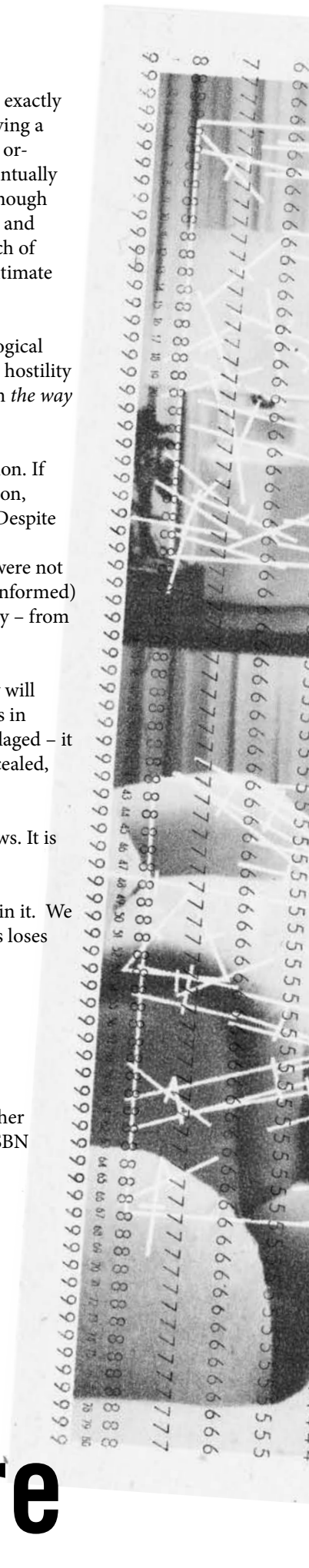
Respond now to what the enemy might do, and science fiction has become a component of military strategy (operating as an escalator). Nowhere is this more dramatically evident than in the work of Hugo de Garis, where a reverse cascade of threat anticipation embeds war in-itself within contemporary information technology.

First implemented in military cryptography machines, and later distributed across robust networks designed to survive nuclear attack, military imperatives have been hard-coded into computational infrastructure from the start. Advanced technology conducts political teleology by adapting C4 systems (command, control, communications, and computation) to the Clausewitzean conditions of intensified war – whether actual or virtual – characterized by extreme escalation, 'fog' and 'friction'. The emergent abstract factor is resilient intelligence, the most flexible (general-purpose) principle of competitive advantage. The crypto-teleology of war (in-itself) becomes increasingly identified with artificial intelligence production.

As a high-level technical theoretician practically promoting the development of artificial brains, Hugo de Garis is implicitly connected to this lineage, despite his avoidance of formal links to military research programs. This distance from overt defense work – which might have lured a less scrupulous intelligence into fantasies of philosophical innocence – prompted de Garis into a conceptual escalation beyond the Clausewitzean framework. Rather than envisaging technology as the conductor of the state war aim, he began to suspect that it was itself an *unsubordinated teleological element*, displacing the state as final cause.

Against the limited conception of a war waged *through* technology, escalated by disciplined science fiction speculations intrinsic to the military apparatus, de Garis turned (through an escalated science fiction) to the model of an unlimited or 'gigadeath' war waged *over* and *about* (while also still through) technology. The fate of technology would no longer be decided by the wars among states, but would itself become a polarizing cause, determining a trans-political war, with states as teleologically-subordinated components (or large-scale technological parts). The point of contention: Will super-human artificial intellects (or 'artilects') be permitted to happen?

The coming Artilect War – "almost inevitable before the end of the 21st century" [2] – subsumes everything into the axis of escalation, pitting 'Cosmist' proponents of technological extrapolation without limit against the 'Terran' resistors who oppose it. The retro-chronic dynamics of escalation are driven to an ultimate limit by fundamental game-theoretic dissymmetry. The Terrans cannot possibly escalate too hard, too fast, because the Cosmists are *aligned with escalation*, and therefore win automatically if the war is prolonged to its intrinsic extreme. The Terrans cannot allow the war to take its time, knowing that anything other than a 'prematurely' concluded war is a Cosmist success. Time pressure reaches its maximum, through the condensation of an absolute threat that is intricately entangled with the means required to counter it.



End Game

Even in an extreme formulation of the de Garis Artilect War, the Cosmists are still a 'side'. While aligned exactly with the inherent trend of war in-itself, they supply it with a recognizable ideological subjectivity, preserving a residue of dialectical intelligibility. Artilects are double counted, at the bottom and top of the teleological order – as mere weapons, and as final causes. Simply tracking the tangled circuitry of this model would eventually describe complexities beyond pursuit. What can already be comprehended of the Terran perspective is enough to demonstrate that – for the human resistance – it cannot begin quickly enough. If tomorrow is too late, and yesterday none too soon, it crashes through the present to embed itself deeply within the (apparent) epoch of Clausewitzean war. With no Cosmists to represent the cause of escalation, war's crypto-teleology – the ultimate enemy – hides itself among the cross-currents of state-political antagonism.

The question then arises: is Stuxnet a soft-weapon fragment from the future war? When its crypto-teleological significance is finally understood, will this be confined to the limited purpose assigned to it by US-Israeli hostility to the Iranian nuclear program? Does Stuxnet serve only to wreck centrifuges? Or does it mark a stage on *the way of the worm*, whose final purpose is *still worm*? Are Cosmists even needed to tell this story?

The answer depends upon the limitation of war, which can be represented by the proxy of anti-proliferation. If state-political objectives are able to subordinate – or indefinitely master – the crypto-teleology of escalation, then Stuxnet will have 'always been' an instrument of policy, or never significantly more than a weapon. Despite the 'fog' of war, the 'friction' of unpredictable events, and the tendency to techno-military escalation it demonstrates, there would be no reason to think a more-or-less exhaustive explanation for its existence were not already available in *principle*, however deeply encrypted. Then we could know, even if (befogged and disinformed) we concretely do not, that it was designed to prevent escalation – in the guise of Iranian nuclear capability – from escaping the politically-circumscribed order of the world.

If, on the contrary, war is going to escape, then nothing we think we know, or can know, about its history will remain unchanged. State-politics will have been the terrain in which it hid, military apparatuses the hosts in which it incubated its components, antagonistic purposes the pretexts through which – radically camouflaged – it advanced. Its surreptitious assembly sequences would be found scattered backwards, lodged, deeply concealed, within the disinformational megastructure of Clausewitzean history.

"War is god" asserts Cormac McCarthy's Judge Holden. It has its own order of providence and its own laws. It is the ultimate meaning of things.

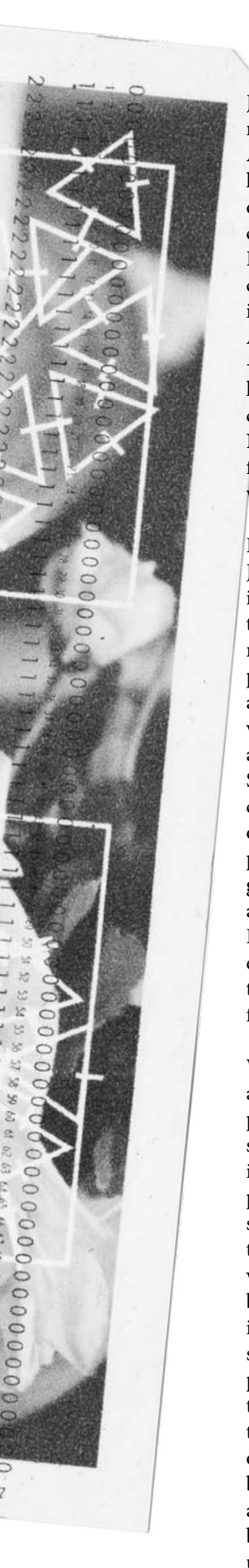
We are under no compulsion to believe a self-declared fiction, or to listen uncritically to a character within it. We have only to think about the ways things hide, or – less demandingly still – to accept that thoughtlessness loses wars.
Does the war think? We don't know (but the idea sounds insane).

[1] On War, by General Carl von Clausewitz, translated by Colonel J.J. Graham, http://www.gutenberg.org/files/1946/1946-h/1946-h.htm

[2] Hugo de Garis (2005). The Artilect War: Cosmists Vs. Terrans: A Bitter Controversy Concerning Whether Humanity Should Build Godlike Massively Intelligent Machines. Palm Springs, CA: ETC Publications. ISBN 0-88280-154-6.

Museum of Malware

John Menick



January 19, 1986: Brain, the first personal computer virus—or more specifically, the first MS-DOS virus—is released into the wild. The authors are two Pakistani brothers from Lahore, Basit Farooq Alvi and Amjad Farooq Alvi, medical software engineers, who later say their intentions were innocent, just a test to see what would happen. They are telling the truth, presumably, because the authors include their names and address in the virus, discoverable if you know how to use a hex editor. Copyright, byline, a physical address of origin, a company credit, and a warning: Beware of this *VIRUS… Contact us for vaccination*. The boot sector of a floppy disk is Brain's host, the boot sector being the sector that permits a computer to load software into memory. The virus copies itself from the boot sector of the floppy to the PC and then back to another floppy when a second floppy is inserted into the drive. A pure virus, a replicator, nothing harmed or changed, copying across boot sectors.] Appropriately, Brain starts in a hospital]computer, and from the hospital it is carried on five-inch floppy disks —this is before the World Wide Web—aided by cheap airfares and a globalizing white collar labor force. It moves hand to hand, in briefcases, through airports, offices, alongside seasonal colds and flus,infecting high school computer labs and home offices and corporate headquarters. There is no virus protection yet, no McAfee, no Norton Antivirus; and within a few years, the phone calls come in for the brothers, long distance mostly, asking for the antidote to Brain. The brothers help; they say there is nothing to worry about since Brain is only doing what all viruses in essence do: replicate.

Replication without a partner, *self-replication*, a concept first modeled in the late 1940s by mathematicians John von Neumann and Stanislaw Ulam. Given a grid of cells—cellular automata—and a number of simple instructions, one can create an abstract machine that copies each of its parts to new a location along with the original set of replication instructions. The original designs also include more literal versions of these machines, and later scientists expand on the concept, proposing self-replicating spacecraft and factories, prototyping machines and robots. Working from these ideas, in 1961 Robert Morris Sr., Victor Vyssotsky and M. Douglas Mcllroy create a program at Bell Labs called *Darwin*, in which dueling computer programs vie for control over a sector of memory called an arena. Eventually an unbeatable predator program emerges, an apex to the pyramid (as well as the eventual inspiration perhaps for Tron's Master Control Program). Several variations on Darwin and a decade later, Bob Thomas writes both the first computer virus and the first computer worm, Creeper. Like much in computing, fiction leads science: the term worm itself comes from one of the earliest examples of cyberpunk fiction, John Brunner's *Shockwave Rider*, in which a fugitive phone phreaker, Nick Haflinger, uses a computer *tapeworm* to protect information from snooping corporations and governments. Outside of sci-fi political allegories, a *worm* is a variation on a virus, though in addition to being able to replicate, a worm can also transport itself across networks—no need for floppy-to-floppy transmissions. Like Brain, Creeper is harmless, but it also is a pest, and quickly a second program, Reaper, is written in order to eradicate it. The dynamic between Reaper and Creeper can be modeled along the same lines as participants in the Darwin game—emergent predator-prey dynamics—and, as the name *Darwin* suggests, programmers were fully aware that these automated programs had qualities of life—however *life* is defined.

When reading the literature on biological viruses, it is striking to see that the scientific community is divided as to whether a biological virus is alive at all. A biological virus is not a cell; it lacks the cell's organelles that make proteins and generate energy. A biological virus is a protein wrapping DNA or RNA; a design, if that is the word, so simple that scientists cannot reach a consensus as to whether a virus is alive or dead. Instead of *living thing*, instead of *nonliving thing*, in some scientific literature viruses are described as *on the edge of life*. A vague phrase, *the edge of life*, raising images of shuffling undead, a twilight Interzone. But biological viruses are not so romantic, not so unknown. They are closer to what Descartes thought of animals: machines, clockwork things that can only remake themselves. Since viruses are not cells, since they lack many of the properties of life, the virus must bind to a host cell's surface, and if by luck the receptor on the surface of the host cell can be opened by the virus and the virus is welcomed in, then the host cell's machinery is available for the taking. The rest is coding: with a cell's genome factory hijacked by the virus, the cell inadvertently produces more viruses, sometimes so many in quantity that the host cell itself may die, broken up by its new multiplying guests. The process is fast, with viruses reproducing in hours and days, and in each quick generation comes mutations in the virus's genetic sequencing. Many of these mutations are harmful to the virus and many do nothing at all for the virus. But some may help, giving the virus accidental selective advantages, such as defenses against immunity, or more virulent reproduction capacities, and the virus thrives and moves on. It is difficult to say whether or not biological and computer viruses are analogous, whether Darwin the game and the process of natural selection are operating under the same principles. Or, to put it another way, it is difficult to say whether or not viruses, biological or electronic, are simply two kinds of automated interactions, and whether life, however it is understood, is little more than mechanical theater.

Corruption of blood: an English legal term describing the inability to inherit property, usually due to some capital crime committed by the inheritor. A defunct concept, now abolished in both the US and the UK, one finds *corruption of blood* unexpectedly in World of Warcraft, a high-tech game whose sole content is fantastic pre-modernity. Released in 2004 by Blizzard entertainment, World of Warcraft (WoW) is a *massively multiplayer online role-playing game* (MMORPG), in which millions of men and women play one another for pleasure and profit. WoW is a typical fantasy landscape, with touches of science fiction and steampunk, where druids, priests, rogues, warriors and other classes undertake quests and battles with complex and not always predictable outcomes. As is the case when a WoW deity named Hakkar the Soulflayer is introduced as the leader of Zul'Gurub dungeon. Controlled by the game's artificial intelligence, Hakkar is a vampire who, among other talents, drains attacking players of their blood to replenish his own health. The game's programmers also provide Hakkar with a spell, or *debuff*, called *corruption of blood*, which temporarily contaminates an avatar's blood, sapping it of some life. This spell can also provide protection against Hakkar's vampiric algorithm. Infect one's avatar with the spell, and Hakkar will harm itself when drawing the avatar's blood. The spell has a second property, new to the WoW universe: it can be spread from avatar to avatar through proximity, thus taking on the properties of a virus. If a healthy avatar walks close enough to an infected avatar, there is a one hundred percent chance that the healthy avatar will become infected. At first, as planned, Zul'Gurub dungeon acts as a quarantine, containing the spread of the virus to players and their pets, but it is these pets, *hunter pets*, that provide a viral inter-species link to the outside world. The pets—like Hakkar, also algorithmic creations—could be dismissed by players back to cities outside of the dungeon, where the pets, asymptomatic like real world vermin might be, spread corruption of blood to thousands of players. Worse, player's avatars can also teleport from the dungeon back to main cities, carrying corruption of blood back to innocent populations. Very quickly a virtual, worldwide pandemic is born. This event is unintended by the game's designers, and the spell quickly spreads to other AI-controlled characters and weaker, less healthy players. The weaker characters immediately begin to die, and after a short time some players resign, while many players maliciously help the disease spread, and others attempt to help infected avatars. Since WoW is a virtual world and resurrection is possible, the virus becomes more of a nuisance than an apocalypse. Blizzard resets the WoW servers, instantly ending the plague, but soon several epidemiologists take interest. In *The Lancet Infectious Diseases*, Eric T. Lofgren and Nina H. Fefferman propose using MMORPGs to study the behavior of citizens when faced with an epidemic. As they write in their article, computer software like Transport Analysis Simulation System and Epidemiological Simulation System rely on cellular automata, historical data, and predicative modeling to guess behavior in an epidemic situation. Given the need for large populations of participants and geographic scale—plus inherent ethical limitations—actual, real-time reactions of a population to a disease outbreak cannot be modeled with any accuracy, unless one were to use an already existing community like WoW's. The authors note that the corruption of blood incident *marks the first time that a virtual virus has infected a virtual human being in a manner even remotely resembling an actual epidemiological event.*

The stated purpose of danooct1's YouTube channel, *Computer Viruses in Action, is to entertain users with the effects of (mainly older) pieces of malware, while educating them as to how they work.* To date, the channel has 22,292 subscribers, and its videos have been watched 7,466,520 times. According to a Twitter account with the same handle, danooct1's real name is Daniel White. He writes 8-bit music and tests computer viruses for fun. danooct1 cannot send you any actual malware because this would be against YouTube's terms of service. He also does not accept unsolicited Steam or Skype friend requests. In each of his videos, Daniel White demonstrates a malware infection on an operating system or program. The operating systems are usually obsolete, and the malware is, as expected, difficult to obtain. Most of the videos are titled with the same labeling system: first the type of malware (worm, virus, Trojan, etc.), followed by a period; then the target operating system or program (DOS, Win32, Microsoft Word, etc.), followed by a period; then, finally, the name of the malware. Names include: Savior, Rigel, Gruel, Color Bug, Gigger, Melissa, Prizm, Selectronic, Phrase, Ari, Fagot, Prolin, Artic Bomb, Apparition, and Acid 2. The most popular species of malware is the virus, and DOS is among the most popular targets. Like an enthusiast of American Civil War rifles or Soviet space gear, White's YouTube channel is devoted to the morphological variations within a category of technology. There is little or no discussion of code, almost no technical jargon. Instead, the infected desktop is shown as a kind of proving ground—an Aberdeen for the security enthusiast. White triggers virus after virus, with each example announcing its arrival in paroxysm of 8-bit graphics and bitmapped clipart. Viruses now are fully weaponized, malicious. This is because viruses have become profitable, and as their creators use them to steal data and survey hosts, it's no coincidence that viruses improve drastically in technical variety and quality. Monetized and lethal, their development mirrors that of predatory capitalism, where shorter product cycles are used as a way to increase profits and to drive technological innovation. Building the most innovative phone, or at least convincing the public you have done so, and selling a new edition of that phone every year to the same consumers, makes you the richest company in the world. Build the fastest and most lethal virus, and the most innovative virus designer will make the most money as well. There is, for example, *ransomware*, software that holds a user's data hostage until a fee is paid to a hacker. And there are better-known *Trojans*, software that hides and waits on a computer's hard drive until called upon to act as a part of a botnet, a distributed network of compromised machines rented out by criminals to the highest bidder. Malware's evolution, cultural and perhaps Darwinian, has led to a great variation of types and techniques, and when looking through the online databases of McAfee or Norton or danooct1, one can't help but think that these warehouses of malware species constitute a kind of museum. Not unlike a natural history or military museum, these catalogs are concerned with the variations of a life form or tool; their aesthetic complexity is as specialized as a breed show. And to compare them to American Civil War rifles is not a loose analogy. Malware has become a category of munitions, designed by intelligence agencies, mafias, terrorist organizations, mercenaries, and governments to not only steal credit card information and computing cycles, but also to destroy enemy machines and workers. The best example of this is Stuxnet: malware most likely developed by American and Israeli intelligence agencies, that targets the Siemens industrial software used by Iran's nuclear program. Stuxnet, another worm, is the most sophisticated piece of malware developed to date. Discovered in 2010, Stuxnet's travel itinerary involves Iran, and its operation is intended, most likely, to be contained to nuclear-related facilities. But after it is released, an error in the worm causes it to spread beyond these specialized host machines, leading to its discovery by Iranian engineers. Stuxnet is designed to destroy the centrifuges used by Iran to enrich uranium; the worm spins the centrifuges out of control, damaging or exploding them, thus making the worm one of the few examples of malware that could cause harm to human beings. An order of magnitude larger than anything previously known, Stuxnet is, perhaps, a program on the edge of life, one that can cross from the symbolic logic of computer software to the murderous logic of international politics.

David Harley in conversation with Lars Holdhus

David Harley CITP FBCS CISSP

LH: Stuxnet made us aware on how technology can be made use of in targeted attacks on infrastructure systems. What do you see as possible outcomes of attacks from malware similar to Stuxnet?

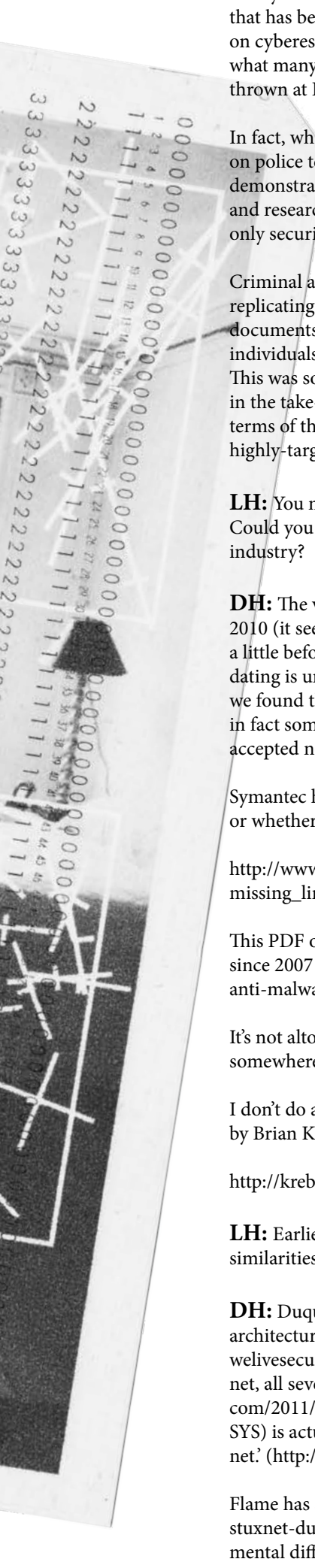
DH: I agree that Stuxnet was something of a game-changer in terms of the public and media visibility it brought to the potential of infrastructural attacks. However, discussion of SCADA, ICS and infrastructure-related attacks (potential or actual) was already taking place among security and SCADA specialists when I became interested in the field, and obviously there have been attacks that haven't attracted the same level of interest.

- The Siberian pipeline explosion in 1982, is alleged to have been caused by a CIA logic bomb, but the truth of that story has been debated, while the Desert Storm printer virus is usually held to have been a hoax.
- Byzantine Candor 2002 onward, targeting military and government agencies in the US.
- Ghostnet, 2007 onward. Multiple targets, including India's embassy in the US and the offices of the Tibetan government in exile.
- Aurora. Targeted Chinese human rights activists and some big players in the US technology industries, notably Google. Proprietary code stolen, activist emails compromised.
- Shadows in the Cloud, 2009 onwards: Targeted Indian and Tibetan government offices and the United Nations. Sensitive correspondence and documents compromised.
  Note that targeted attacks on Tibetan and other activists continue to this day: in fact, they're the main thrust in OS X–targeting malware currently.
- Night Dragon attacks on petrochemical companies like Exxon, Shell and BP.
- Attacks from Russia on Estonia and Georgia, targeting a range of web sites including government, media and finance organizations.
- Titan Rain: alleged theft of military Intel by China on (Lockheed, NASA, Sandia) Moonlight Maze: also targeted military intel, allegedly, by Russia (Pentagon, NASA, Dept of Energy, research labs)

While there are indeed 'similar' attacks – Flame, Duqu etc., plus the otherwise unrelated malware like Chymine and some Sality variants that seized upon vulnerabilities that Stuxnet was the first to exploit – Stuxnet represented a somewhat unusual confluence of factors:

- A target specific and 'desirable enough to attract the necessary resources for what seems to have been a massive collaborative effort.
- A highly specific payload requiring highly specialized knowledge both to build and to get to the bottom of when the malware finally tripped alarms in the anti-malware industry.
- The availability of several unknown zero-day vulnerabilities (and the capacity for seeking them out).
- The availability of a parallel and hard-to-fix weakness in the Siemens ICS environment. Not only did the backdoor apparently require serious re-engineering by Siemens, but ICS-targeting malware almost by definition presents operational difficulties in addressing on site even where patches and updates are readily available.
- Targeting a region where political considerations militate against the strict observance of licensing requirements for software from outside the region. This creates an environment somewhat isolated from the mainstream communication channels between vendor and client software, and it's interesting to speculate on how much longer the malware might have remained under the radar if it had not also been picked up in regions that weren't affected (or less affected) by export/import restrictions.
- Use of stolen certificates at a time when malware was far less likely to take that approach, which wasn't particularly taken into account by some security products at that time.

I'm by no means saying that such a combination of factors can never occur again. In fact, if there's one thing that has become very clear over the past few months, it's that governments can always find resources to spend on cyberespionage at home and abroad: while there is far less discussion of cybersabotage and other facets of what many people call cyberwarfare, it would be naïve to think that the kind of resources that seem to have been thrown at Iran's nuclear industry couldn't be found for other targets.



In fact, while some of the speculation about how modified Stuxnet code could perform all manner of attacks on police telephone networks, hospital systems and so on, were close to fantasy, there's no doubt that it did demonstrate how successful a targeted or semi-targeted attack can actually be given a sufficiency of resources and research, and a similar 'tiger team' approach to quite different targets could probably be as effective. It's not only security researchers who learn from experience and evolve into other techniques.

Criminal and nation-state funded malware developers have generally moved away from the use of self-replicating malware towards Trojans spread by other means (spammed URLs, PDFs and Microsoft Office documents compromised with 0-day exploits, and so on). Truly targeted non-replicating malware (aimed at individuals, often using customized social engineering as well as customized code) is much harder to catch. This was so before Stuxnet, of course, but the Stuxnet family's perceived success has certainly had an influence in the take-up of similar stealth techniques by other state-sponsored malware. It's also had knock-on effects in terms of the take-up of technologies that are seen as more effective than conventional anti-virus in countering highly-targeted malware.

LH: You mention that Stuxnet went under the radar before it was discovered in the anti-malware industry. Could you give me an estimate on when it was created and how long it took before it surfaced in the anti-malware industry?

DH: The version that kicked off the fuss after it was announced by VirusBlokAda was identified in June/July 2010 (it seems much longer ago!). We did notice after the announcement that we'd been detecting it generically a little before that, but of course we had no idea about the implications of that detection up until then. Precise dating is uncertain, though. Kaspersky estimated that that particular variant started to spread March/April, but we found that the driver MRXCLS.sys was time-stamped 1st January 2009. Time-stamps can be unreliable, and in fact some malware we see is clearly intentionally mis-stamped, so don't take that as gospel, but it's generally accepted now that it might have been around in2009.

Symantec have claimed that a version they call 0.5 existed much earlier (2007) but it's unclear to how far it spread or whether it was able to deliver a payload. Interesting bit of viral archaeology, though:

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf

This PDF offers some interesting insights on the development of Stuxnet. If a version of Stuxnet was circulating since 2007 it took quite some time before it was recognized as targeted malware. Except from reports by the anti-malware industry, when was the first news report on the malware published?

It's not altogether clear to me whether it was circulating in an 'in the wild' sense. It was almost certainly out there somewhere in 2009, though.

I don't do a lot of media-watching, so maybe I'm not the best person to ask, but the earliest report I know of was by Brian Krebs, on 15th July 2010.

http://krebsonsecurity.com/2010/07/experts-warn-of-new-windows-shortcut-flaw/

LH: Earlier in the conversation you mention Flame and Duqu as malware related to Stuxnet. What are the similarities between Stuxnet, Flame and Duqu?

DH: Duqu is similar enough to Stuxnet that we believe it was built from the same source code. It's not only architecturally similar, but the same classes and structures were used to compile Stuxnet and Duqu. (http://www.welivesecurity.com/2011/10/25/win32duqu-its-a-date/) While Duqu implements fewer RPC calls than Stuxnet, all seven of the calls it does implement are found in both examples of malware. (http://www.welivesecurity.com/2011/10/28/win32duqu-analysis-the-rpc-edition/) F-Secure observed that 'Duqu's kernel driver (JMINET7.SYS) is actually so similar to Stuxnet's driver (MRXCLS.SYS) that our back-end systems actually thought it's Stuxnet.' (http://www.f-secure.com/weblog/archives/00002255.html)

Flame has similarities in concept and, arguably, targeting (http://www.darkreading.com/attacks-breaches/stuxnet-duqu-flame-targeted-illegal-wind/240002364). In terms of binary analysis, though, there are some fundamental differences. http://www.welivesecurity.com/2012/07/20/flame-in-depth-code-analysis-of-mssecmgr-ocx/

Eugene Rodionov looked at the similarities and differences between Stuxnet, Duqu, Flame and Gauss in some detail: http://www.welivesecurity.com/2012/08/15/interconnection-of-gauss-with-stuxnet-duqu-flame/

LH: How do you and ESET relate to the ethics surrounding nation-state funded malware?

I can't speak for ESET on that. However, my own opinion is that it's far from unreasonable for an AV company to cooperate with a government or law-enforcement agency where it's a matter of national security or a criminal investigation, even if there is no legal compulsion. But blanket non-detection an object known to be used (however legitimately) by a government agency would be ethically problematical. Not because the AV industry is anxious to give comfort to criminals and terrorists, but because of the risk to the community if 'legitimate' malware were to be misused. (Either by a malicious third party or because of inappropriate use by the agency that 'owns' it.)

LH: Is there a difference between nation state funded malware and criminal funded malware?

DH: There's certainly a case to be made for a difference in intent. However, intent isn't generally measurable by automated detection. It was maybe easier in the days when most malware was viral. You could mostly assume that if it incorporated self-replicative code, it was viral and that would make it malicious. The kind of non-replicative activity that might constitute a payload is often far more equivocal. For example, a program that formats a disk or allows access to a remote service could be legitimate or malicious: it depends on intent. Even when lab analysis ascertains that a file is spyware or a remote access tool doesn't necessarily tell us why it was planted or by whom. For that, you usually need direct forensic investigation of a compromised system, unless it's a more-or-less untargeted, generic attack like most widespread malware.

LH: Earlier you mentioned that there are several facets of what people refer to as cyberwarfare. Could you give some examples of different facets of cyberwarfare?

DH: To be honest, I don't think we're seeing real cyberwarfare. Maybe some rough equivalent of the Cold War... It seems to me that the term has been applied indiscriminately to a range of activities whose non-cyber equivalents aren't considered only to take place during wartime. Not only sabotage, but surveillance, subversion and espionage, terrorism and even civil espionage and cybercrime. While there is an abundance of incidents that suggest all too many politically-motivated conflicts, I'm not convinced that these add up to a form of all-out malware. It could also be argued that governments have muddied the waters by using the label to cover this range of activities in the hope of making them more palatable to populations increasingly worried about erosion of civil liberties and individual privacy.

LH: That's an interesting take on the term Cyberwar. As technology gets more complex and malware follows the same direction it seems that only a few individuals can follow this development. How can an individual citizen protect him/herself from government funded malware?

DH: Well, to paraphrase Schneier, if a heavily-sponsored intelligence agency wants access to your system and your secrets, it will get it. If surveillance on major corporations and government agencies is so widespread and so easy, what chance do individuals with limited resources have? Well, they do have the advantage of not generally being of interest to government agencies. As opposed to more generic malware, which even if it isn't put out in massive spam campaigns, isn't highly targeted either: the bad guys are just hoping to reach vulnerable people or systems. Much top-level government-sponsored surveillance is also more-or-less untargeted, but is the starting point for finding more specific targets.

That doesn't mean that certain agencies don't have their data and/or metadata, because they almost certainly do. However, they're only going to examine data closely that trips alarms, such as certain keywords in metadata or the suspicion of unusually strong encryption. Not that I'd want to dissuade home users from using better encryption than most of them do, but they can't assume that encryption will keep all their secrets safe. I doubt if using something like PGP would in itself raise a big red flag, but in combination with other indicators might attract attention. Using industrial strength security programs isn't going to do any harm, and we do know that some government-funded malware is caught by anti-malware simply because it has suspicious characteristics, even if we don't always know what it is. And the obvious things like keeping operating systems and applications properly patched. And trying to be resistant to all manner of social engineering, though that's infinitely easier to say than to achieve.

Some good points on this topic made here, by the way: http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance

LH: What you and Schneier are outlining seems quite realistic in relation to what we have seen the last half a year in the news. You also mentioned earlier that citizens are increasingly worried about erosion of civil liberties and individual privacy. What could future scenarios look like if this escalates?

DH: We're already seeing some squirming in countries where much of the population is concerned – and can express its concerns – about governments spying on their own people. In general, people are less concerned about their own nation spying on people of other nations – understandable in a paranoid, terrorist-fearing environment – but worried about the encroachment of the state into their own privacy. Hence, perhaps, the frequent governmental conflation of cybercrime and cyberterrorism. You're obviously as aware as I am of the increased focus of digital awareness/liberties groups on this area of governmental activity. While this is understandable and in many respects acts as a necessary restraint on unwarranted government activity, it can result in a pressure group that assumes a self-defined authority that isn't matched by its effectiveness and understanding of all the issues, and that is likely to lead to confusion more generally.

As more people become aware that the internet is a lot less safe and infinitely less private than they may have thought, there's likely to be more use of low-end security products and services, especially those offering some form of encryption. Since many people won't be able to distinguish between good free or cheap products and snake oil, there's likely to be a surfeit of poor advice and a sense of false security. It's ironic that a lot of advice is coming from the same agencies whose surveillance activities are causing so much concern. Clearly, this may be seen as damaging its credibility even though some of the advice given may be quite sound.

In criminal and governmental circles, there's probably already a better understanding of what I expect someone has already called cybercamouflage, and perhaps a welcoming of expanded business opportunities. We're already seeing more products and services related to personal security and privacy of little or no real value, and social engineering used by phishers and distributors of malware also based on exploiting the victim's paranoia and yearning for safety.

LH: Recently there's been some experts suggesting that there might be planted backdoors in hardware from Intel and AMD. Some years ago the US State Department decided to ban Lenovo Hardware from their classified work. Could you give some insight into the hardware side of Cyber attacks?

DH: You mean the claims by Steve Blank? Well, yes, there might - you might want to ask someone from McAfee about Intel backdoors ;-) - but the fact is that it's just speculation. It sounds like a PR exercise to me.

The State Department banning Lenovo hardware does at least have some obvious logic: it's not ridiculous in the current climate for one government agency to be concerned about hardware assembled in a nation state with which it has a relationship that can at best be described as ambivalent. It's not as paranoid as the NSA banning Furbies (unless the NSA knew something about Furbies that the rest of us didn't...)

However, there are certainly instances of nation states sourcing (because its economically advantageous) components of their IT infrastructure from other states with whom they have an awkward relationship. And that does raise the possibility of hardware backdoors, but again that's to some extent speculative.
This sort of speculation does go a long way back, though. The Iraqi printer virus for example: http://www.vmyths.com/hmul/7/3/ Or the 1982 Siberian pipeline explosion: http://en.wikipedia.org/wiki/Siberian_pipeline_sabotage