Kleptography

Finn Brunton

> One must remember that mathematics, like death, never makes mistakes, never plays tricks. If we are unable to see those irrational curves or solids, it means only that they inevitably possess a whole immense world somewhere beneath the surface of our life.
>
> Yevgeny Zamyatin, *We*

The settings alone brush perilously close to fiction: a deserted basement in King's Cross in which hard drives are destroyed; a small room, containing only four chairs and a fingerprinting machine, in Heathrow Airport; the offices of covert savants in plinths of black glass, lined with copper to prevent signal leakage; gleaming white geodesic radomes glittering in the sunlight at Menwith Hill and in Australia, far inland at Pine Gap, coordinating signals from spy satellites over a third of the planet; the transit zone at Sheremetyevo Airport; the locked rooms of fibre-optic splitters in telecom buildings; a sunlamp and a maroon couch in a room that is physically in Knightsbridge and legally extraterritorial as a diplomatic mission; two people waiting outside a restaurant in a mall in Hong Kong for a man with a Rubik's cube.

In fact, some of the settings against which the historic disclosure of twenty-first-century state surveillance are playing out echo fiction directly and deliberately. The current director of the National Security Agency, General Keith Alexander, based the design of the Information Dominance Center for the Army Intelligence and Security Command (the AISC, which he headed prior to his appointment to the NSA) on the bridge of the *Enterprise,* from *Star Trek: The Next Generation*.[1] DBI Architects (DBIA), the company contracted for this project, have a 'stealth' practice that specializes in producing these dramatic environments. They have built spaces for Lockheed Martin, the US National Counterterrorism Center, GeoEye – the satellite imagery business used by Google Maps and the National Geospatial-Intelligence Agency – and the remodelled White House Situation Room.[2] (If you saw the picture of President Obama and the national security team looking on during the raid on the bin Laden compound, you've seen DBIA's work.) Their style is one vast homage to Sir Ken Adam, designer of the War Room in *Dr. Strangelove* and numerous Bond villain command centres and secret bases; looking through their portfolio, one awaits the arrival of Roger Moore, jogging in and slaying henchmen. These interiors are like love hotel fantasy suites for geopolitical security services. For Alexander, DBIA delivered the sliding doors, gleaming chrome, central command chair, massive viewscreens and all the rest.

Naturally this is somewhat hilarious, with the hydraulic-hissing doors and thin science-fictional veneer – those contoured consoles enclose ancient CRT displays, beige keyboards, and database management software. It is also a brilliant bit of political scene-setting. In his time as head of the AISC, Alexander had many people to impress and political battles to win in order to rise to his current position, and bringing them aboard the *Enterprise* to sit in the captain's chair helped smooth the way. Alexander is famous, as career political appointees go, for a kind of genial, unflappable charisma,

particularly when articulating his steadily growing signals intelligence demands to computer-averse members of the US government and military. Letting his visitors play Captain Picard for a few minutes and watch the action on an updated Strangelovean Big Board was part of that capacity. The Information Dominance Room in Ft Belvoir, Virginia, was – as its name implies – one in a long line of chambers of political seduction, from Talleyrand's carefully selected statuary to the looming Fascist offices, vast spaces for the theatre of intimidation and submission, parodied by Bertolucci's *The Conformist*.

Theatre of security

These are sets, in other words, and to their scenography we can add performance – an infinitely more refined version of what is called 'security theatre', played out in registers of arrogance and presumptive omniscience, withheld secrets, cryptic allusions and threats both direct and indirect. Consider as a theatrical act the requirements exacted by the NSA from IBM for the company to work on a particular set of encryption systems (the S-boxes, using the Data Encryption Standard, in the 1970s): not merely to keep all the development documents numbered and locked in separate safes, but to hold briefings for NSA visitors who would sit, taking notes and evaluating in perfect silence on behalf of a project whose requirements for secrecy were themselves secret.[3] Or the protest by NSA employees in a meeting of an international mobile telephone standards committee: any discussion of certain secure protocols for encrypting mobile phone activity would violate export control laws, and the discussion could only proceed after all the non-US nationals had left the room (to reiterate, this was an *international* mobile telephone committee). This paralysed the conversation and left mobile phone encryption up to 'a clueless Motorola employee'.[4] Or, of course, the theatre of intricate riddling language beloved of NSA employees obliged to give testimony and White House flacks to address the press: use of tenses – 'is not and will not monitor [Chancellor Merkel's] communications' – intricately slippery turns of phrase ('collection,' 'subsequent processing', 'inadvertent', 'incidental', 'content'), and of course Director of National Intelligence James Clapper's masterpiece of an answer

to a question about US domestic surveillance in a Senate hearing in March: 'No… not wittingly.' (Which, as it turns out, means 'Yes'.)[5]

But the high point of the theatre of security is not in the play of secrecy and evasion, but in the performance of total knowledge and information dominance – in the work of salesmanship, both inside and outside the apparatus of government. We now know in some detail the sorts of presentation Alexander would make to others in the US intelligence community, structured around what his detractors called 'BAGs', or 'big ass graphs'. These vast tangles of boxes and arrows extruded from intercepted metadata, purporting to describe various networks of insurgents and terrorists, are immediately recognizable in description: the work of the glad-handing big data huckster with an analytics package to sell you, a great heap of good-looking chaff blown up and colour-coded on a slide.[6] Along with tales of monstrous attacks averted, somehow always difficult to pin down precisely, these constitute the display of 'cyber command', to take a term from another of Alexander's projects, and arguments for why he and his political fiefdom should be given further monitoring capabilities.[7]

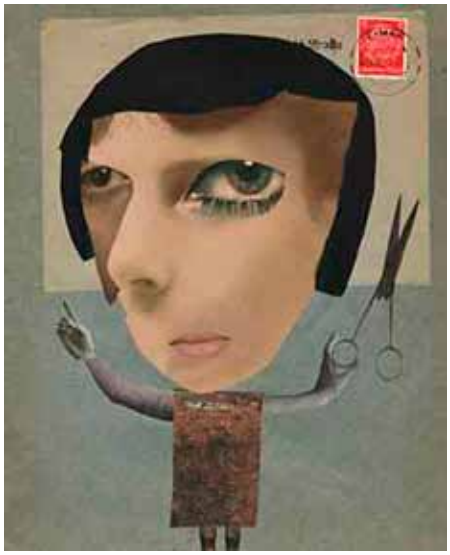
It may seem flippant to dwell on things like scene-setting, performance and aesthetics in the midst of the various unfolding diplomatic, civil and political crises unleashed by the Snowden documents. There is already so much of grave consequence to discuss. Choose your historically emblematic moment: the announcement of plans for parallel Internet infrastructures, and financial penalties that route around the United States and its UKUSA/'Five Eyes' agreement partners; the Google engineers 'exploding in profanity' on seeing the slide that revealed how thoroughly their systems had been compromised; the Montevideo Statement to globalize the governance of the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Assigned Numbers Authority (IANA).[8] We could continue in this vein. And yet attending to the aesthetics matters, both at a theoretical and a practical level.

When I wrote about Wikileaks and the Assange archive for *Radical Philosophy* two years ago,[9] I drew on the temporality of encryption, the way it conflates speeds both faster and slower than the limits of human experience. At the heart of much Internet security lies the factoring of semiprime numbers into the two large primes of which they are the product. Given a long semiprime, determining the two constituent factors by brute force will take time on the scale of millions of years.[10] Given another semiprime which shares a factor with the first, the operation takes a matter of microseconds. (Blinking your eyes as you read this is a comparatively dynastic expanse of hundreds of thousands of microseconds.) Our lives in the long historical present sit roughly at the midpoint between these two speeds, between millionths of a second and millions of years. Amidst the ceaseless wave of revelation, disclosure, crisis and demand for action, it serves us well to draw on the geological slowness embedded in encryption. There is real power in sitting still and thinking patiently, carefully, clearly and for the long term. The impulse is to recommend and advocate particular technologies, cryptosystems and political actions, for urgent response to crisis. Those are valuable, and well worth our support. The chance to think more carefully and patiently is also incumbent on us, however. It is in this spirit that I would like us to return to some of the stage sets for the performance of political seduction and threat with which this essay opened, to comprehend the work they are doing and how that can be counteracted.

Art of secrecy

What is being accomplished by those performances is best understood by expanding on the idea of *kleptography.* This concept was originally quite specific and concrete: black-box cryptosystems, implemented in closed hardware and not available for community review, could have back doors in place that would allow their designers to access the keys or the supposedly secure messages they produced.[11] In discussions over

the last decade-plus since the term was coined, its applications have been expanded. Kleptography is 'persuading the party to be intercepted to use a form of cryptography that the attacker knows they can break'.[12] This broader definition encompasses many different methods of circulating compromised technology, beyond back doors hidden in proprietary systems – methods like threatening or bribing companies, manipulating standards bodies and committees, concealing or classifying vulnerabilities, and intimidating governments and citizens. (Think of it as an anticipatory version of the cruel joke in the crypto-community of 'rubber hose cryptanalysis': decrypting a message by beating someone until they give you the key.) An intuitive example of kleptography as a practice is the post-World War II career of the German Enigma machine, the encoding device employed, in various forms, by the Nazi military and state. Enigma was successfully cracked thanks to the heroic efforts of Polish and British cryptologists (most notably at Bletchley Park), but this highly classified achievement was not widely known until the 1970s. Thus the UK could export the machines abroad to foreign governments, selling as perfectly secure what trusted services among the Allies knew were open devices – which is why there are lightly modified Enigma machines with Hebrew keyboards, passed along to the Israel Defense Forces in 1948.[13] Likewise, the disruption of that mobile phone security meeting, mentioned above, helped to produce the widely deplored Cellular Message Encryption Algorithm (CMEA), the kind of deliberately flawed technology that could be exploited by the agency doing the disrupting.[14] There is a substantial budget item in the NSA 'Sigint Enabling Project,' an initiative to undermine encryption, to 'Influence policies, standards and specification for commercial technologies', which nicely encapsulates the work of kleptography – and notice those verbs, *influence* and *persuade.*[15]



Alan Magee, *Portrait of Hannah Höch*, 1992

General Alexander's sci-fi posturing is part of this work, with the strutting performance of Information Dominance and omniscient awareness, building on the legacies of 1980s and 1990s spy movies and cyber-kitsch to win over politicians and bureaucrats. The reputation and influence of the NSA, with their looming monoliths of Kubrickian glass and capacity for keeping secrets, has apparently made it possible for them to get the notionally impartial National Institute of Standards and Technology (NIST) to sign off on mathematical objects used to generate cryptographic keys which may be deeply compromised – a clever and despicable act of kleptography (and one with historical precedence in NIST's relationship with the NSA).[16] It in no way detracts from the reality of their abilities to point out that part of what the NSA and other agencies have done in the construction of state surveillance has been accomplished by social and political means, by set dressing and scene-setting, by the performance of the theatre of security, by the deployment of surveillance aesthetics. These aesthetics and their power to impress and cow are ripe for deep critique and artistic appropriation, to be sliced open by Hannah Höch's scissors – a process already beginning.

Finally, consider the most powerful form of kleptography, described in a recent Internet Engineering Task Force document: 'A highly effective form of kleptography would be to make the cryptographic system so difficult to use that nobody would bother to do so.'[17] Even better than the work of carefully, covertly back-dooring some piece of communications hardware, just make the available systems so tedious, time-consuming, annoying or opaque to use that people, by and large, simply don't – they send their messages in clear and hope for the best, or try not to think about it. This is the world in which we actually live, and it presents another challenge for critique, for art practice, for design and for aesthetics. The work of security as a way of communicating and a way of

living has much to offer: literacy in hardware, software and infrastructure; an approach to law and spaces of sovereignty, imperial control and freedom; the labour of affinity, community and trust; and areas of mathematics with just as much to offer contemporary philosophy (and more immediate political applications) than set theory. As we put a stake through the heart of the theatrical kitsch of state surveillance, can we make the practice of liberated security as an element of daily life interesting, compelling, exciting and beautiful? Can we make secrecy, our secrecy, into an art?

Notes

1. Shane Harris, 'The Cowboy of the NSA', *Foreign Policy*, 9 September 2013.
2. I refer the reader to DBI Architects' 'Stealth Portfolio', atwww.dbia.com/stealth; although in the days since the publication of the *Foreign Policy* piece, they have set that part of their site to redirect to their main page. However, their PDF concerning the design of the Information Dominance Center has been widely mirrored; a copy can be found at http://finnb.net/rp/dbia.pdf, among other places. We reproduce one image on p. 3 above.
3. Steven Levy, *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age*, Viking, New York, 2001, p. 55.
4. John Gilmore, 'Re: [Cryptography] Opening Discussion: Speculation on "BULLRUN"', Cryptography and Cryptography Policy Mailing List (cryptography@metzdowd.com), 6 September 2013.
5. For tenses, see Noah Barkin, 'Germany Says U.S. May Have Monitored Merkel's Phone', Reuters, 23 October 2013. For choice of words, see the lexicon in Jameel Jaffer and Brett Max Kaufman, 'How to Decode the True Meaning of What NSA Officials Say', *Slate,* 31 July 2013.
6. This lack of substance behind the huge claims for intelligence in data-mining captured signals is referred to by sources in numerous different agencies in Harris, 'The Cowboy of the NSA'.
7. Referring to the United States Cyber Command, which Alexander established and still leads.
8. For routing around the USA and its partners, see Amanda Holpuch, 'Brazil's Controversial Plan to Extricate the Internet from US Control', *Guardian*, 20 September 2013. For the Google exploit, see Barton Gellman and Ashkan Soltani, 'NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say', *Washington Post*, 30 October 2013. For the Montevideo Statement, see ICANN, 'Montevideo Statement on the Future of Internet Cooperation', 7 October 2013, www.icann.org/en/news/announcements/announcement-07oct13–en.htm.
9. Finn Brunton, 'Keyspace: Wikileaks and the Assange Papers', Radical Philosophy 166, March/April 2011, pp. 8–20; http://www.radicalphilosophy.com/commentary/keyspace-wikileaks-and-the-assange-papers
10. This reflects our current public understanding; there are possibilities and rumours of problems in the generation of the numbers, breakthroughs in the process of efficient factoring and new number sieve systems, extremely efficient hardware optimized at the chip fabrication level, and of course prospects like quantum computing, all of which could imply dramatic changes in the timescales required.
11. Adam Young and Moti Yung, 'Kleptography: Using Cryptography against Cryptography', in David Chaum, Christoph G. Günther and Franz Picher, eds, *Advances in Cryptology – EUROCRYPT '97*, Springer, Berlin, 1997, pp. 62–74.
12. Phillip Hallam-Baker, 'PRISM-Proof Security Considerations', sect. 3.4, Internet Engineering Task Force (IETF) Internet–Draft, 11 September 2013, www.ietf.org/id/draft-hallambaker-prismproof-req-00.txt.
13. Friedrich L. Bauer, *Decrypted Secrets: Methods and Maxims of Cryptology*, 2nd edn, Springer, Berlin, 2000. p. 112.
14. Gilmore, 'Re: [Cryptography] Opening Discussion'.
15. Nicole Perlroth, Jeff Larson and Scott Shane, 'N.S.A. Able to Foil Basic Safeguards of Privacy on Web', *New York Times*, 5 September 2013. See, in particular, the annotated budget released as part of this reporting, 'Secret Documents Reveal N.S.A. Campaign against Encryption', www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html.
16. For concerns about the history of NIST and NSA, an excellent place to start is the saga of the Dual Elliptic Curve Deterministic Random Bit Generator, NIST *Special Publication 800–90*, which came under immediate suspicion – suspicion which was confirmed by the Snowden leaks. Nicole Perlroth, 'Government Announces Steps to Restore Confidence on Encryption Standards', *New York Times*, 10 September 2013. For considerably more detail on the concerns about the standard curves, see the slide deck produced by Daniel J. Bernstein and Tanja Lange, 'Security Dangers of the NIST Curves', 31 May 2013, http://cr.yp.to/talks/2013.05.31/slides-dan+tanja-20130531–4x3.pdf.
17. Hallam-Baker, 'PRISM-Proof Security Considerations', sect. 3.4.5.