[2]

Strategic Intervention and the Digital Capacity to Resist

Howard Caygill

What is the character of strategic intervention in contexts where there is a claim not only to a monopoly of the use of the means of violence but also a monopoly of secrecy? What options for resistance are available when the state extends its claim from the monopoly of violence to a monopoly of information? What is the quality and the conduct of resistance—its strategic options—when confronting not only the potential physical violence of state and corporate power but also its *arcanum*, the realm of secrecy and the exclusive control of access to information that it inhabits? Such questions immediately address the case of digital resistance, whether in the use of the

Internet as a means for coordinating resistance or in resistant interventions carried out on the terrain of the Internet. They assume specific urgency when it is understood that the Internet is increasingly assuming the character of an *arcanum*, or place where states and corporations pursue a monopoly of secrecy, which is to say, the goal of denying us our secrecy. What is a strategic intervention in a context where the state's claim to monopolize secrecy or access to information necessarily entails the surrender of any such claim on the part of civil society?

Arcana and the Internet

For some, the classic example of a strategic intervention in an *arcanum* is the Second World War. Once the *arcanum* of German and Japanese control and command—the Enigma coding of military communications—had been compromised by the work of Alan Turing and other cryptographers at Bletchley Park (Erskine and Smith 2011), what were the strategic options available for effective intervention? The obvious option was to use the information gained by the breach of military secrecy to secure short-term military advantage: if you know where the U-boats are you warn the ships in the convoys; if you know where enemy forces are and their intentions, you intervene in a pre-emptive response. But such intelligence-directed interventions would immediately alert the enemy that you had broken their codes—entered their *arcanum*—and they would respond by reconfiguring their codes. Another strategy consists of the selective and even disguised use of the information, intervening under the cover of fictions (spies sent and sacrificed, spies invented, bodies floating in the sea bearing false secrets), all designed to prevent

the enemy from suspecting that their monopoly of secrecy had been compromised and their codes broken. In this case, strategic intervention becomes a play on appearances—giving any other explanation for operational knowledge than the real one. But this also entailed massive sacrifice—deliberately losing battles, only intervening when the secret of knowing the enemy's secrets is not risked. Neal Stephenson's novel *Cryptonomicon*—published in 1999 and widely read within the hacker community—fictionally elaborates on the scenario that the Second World War didn't happen but was a fiction, a cryptonomicon or fictional intervention in the *arcanum*. However extravagant the fiction, it remains the case that the field of operations research in the 1940s was close to the *arcanum* and many of its personnel—John von Neumann, Turing—would be crucial in the pre-history of the Internet.

Why Assange Missed the Point

In his 2012 dialogs *Freedom and the Future of the Internet,* Julian Assange referred to the "militarization of the Internet," or the "tank in your bedroom," "the soldier under the bed." For him "the Internet, which was supposed to be a civilian space, has become a militarized space … [and as] the communications at the inner core of our lives now move over to the Internet … our private lives have entered into a militarized zone." "We can't see the tanks," he concludes, "but they are there" (Assange et al. 2012, 33). This view contributes to his skepticism concerning the emancipatory potential of the Internet, his view that the possibilities for resistance that it offers are narrow and precarious. Referring to Egypt, but we could now add Turkey, Hong Kong and the United States itself, he warns that digital resistance is a high-risk gamble that once ventured, has to prevail "because if it doesn't win then that same infrastructure that allows a fast consensus to develop will be used to track down and marginalize all the people who were involved in seeding the consensus"—the "critical participants." But how to win in this *arcanum* where the odds are not in favor

of resistance: What would it mean to intervene strategically? Assange's almost intuitive response is to expose and protect—to expose the *arcanum*, state, and corporate secrecy at the same time as protecting his own and his whistleblowers' secrecy by intense cryptography.

Assange's skepticism is a salutary warning to any attempt to mount a digital resistance, but it is important to reflect further on its central premise regarding the "militarization of the Internet" and its implications for an understanding of the limits and possibilities of resistance. My reflections will return obsessively to Carl von Clausewitz and his posthumously published *On War* of 1832 (von Clausewitz 1832–1834); Clausewitz is a central figure both for the development of the Internet and for assessing its potential for resistance. Is Assange right when he says that the Internet "was supposed to be a civilian space" but is becoming militarized? Is it not well known that it was always militarized and that its civilian uses were an accidental exception—space wrested from the military, or conceded by it…? It is, but without really appreciating the gravity and implications of such knowledge for the capacity to resist, prime among which is that if we move in a space that is a militarized *arcanum*, then our actions have to be guided by the appropriate rules and precautions: strategy.

Clausewitz's War of Resistance

Clausewitz is central to the elaboration of a modern theory of resistance. In spite of its title—*On War*—his posthumously published masterpiece is less about war—*Krieg*—than resistance, *Widerstand*, or more precisely the war of resistance. *On War* is not so much an analysis of war than an account of how to resist the emergent military strategy of the revolutionary nation state—France—through what the Peninsular War had called the "little war" or guerrilla, as opposed to the *grand guerre* conducted by the revolutionary armies. From the outset, Clausewitz offers a conceptual refinement that still in many ways eludes current

strategic discussion around the theory of resistance; he is interested above all in the capacity or ability to risk resistance—*Widerstandsfähigkeit*—and not just its performative eruptions. Already on the first page of his first chapter, he defines the two objectives of war as: compromising to the point of destroying the enemy's capacity to resist while enhancing your own. As an idiosyncratic Kantian, his categorical imperative might be phrased, "act so that maxim of your actions enhances your own and compromises your enemy's capacity to resist." The rules for ensuring the survival and enhancement of this capacity are what constitute strategy for Clausewitz—it underlies his specific and historical discussion of the disposition of forces and of tactics. It is basically temporal in that it involves the survival or enhancement of the capacity over time—and in pursuit of the strategic aim of enhancement permits tactical retreat and evasive action. Furthermore, Clausewitz's account acknowledges the centrality of information (and misinformation) for preserving or enhancing the capacity to resist, and in particular the maintenance of secrecy. It was this view that earned him the admiration of Marx, Engels, Nietzsche, Lenin, Mao, Guevara and most recently perhaps his closest and most successful exponent, Nelson Mandela.

But Clausewitz was not only read by the left, his work was also central to nuclear strategy in the Cold War, on both sides, but especially in the emergence of strategic discussion during the 1950s in the United States. There were two opposed positions. On the one hand, nuclear deterrence originally formulated by the mathematician John von Neumann and pursued by President Eisenhower, and on the other, a neo-Clausewitzian position emphasizing survival and the enhancement of the capacity to resist. The latter position was associated with the RAND Corporation and its most prominent exponent was Hermann Kahn, who detailed its execution in an influential theoretical text *On Thermonuclear War* published in 1960. Kahn argued in internal RAND Corporation papers and publically in his book that the prime strategic objective should be less the avoidance of

nuclear war than the enhancement of the possibility of survival and the continued existence of a capacity to resist or, in terms of operations theory, the means of ensuring continuous command and control. His underlying premise was that strategists should prepare the option of launching nuclear war with the security that the capacity to resist would survive a first or retaliatory strike.

Kahn's Resistance after Nuclear War and the Invention of the Internet

Kahn's bringing Clausewitz's *On War* into the nuclear age as *On Thermonuclear War* gives an invaluable glimpse into the quality and range of discussions in the RAND Corporation during the 1950s. He focused on the strategic options available under a "post-attack" scenario, advocating in the name of the RAND Corporation a series of pre-emptive measures to ensure the survival of the capacity to resist after a nuclear attack. He lays out a program of strategic planning dedicated to ensuring the survival of the United States but most importantly of its capacity to resist in a post-attack environment:

> Our study of non-military defence indicated that there are many circumstances in which feasible cultivation of military and non-military measures might make the difference between our facing casualties in the 2–20 million range rather than in a 50–100 million range (Kahn 1960a, 98).

The non-military measures include what will later be known as "civil defense"—fall-out shelters etc.—while the military measures focus obsessively on assuring the survival of the "command and control" structure vital to order, sanction, and execute a counter-attack. A pre-emptive strike on the part of the USSR is assumed to be directed against "command and control arrangements" in order to disable any possible counter-attack. Kahn predicts that "the bulk of their blow will be directed towards destroying, crippling or degrading the operation of our retaliatory forces"

(Kahn 1960a, 165–166) and in particular the system of command and control. He returns repeatedly to this vulnerability, which he describes as the "Achilles' heel" of current strategic doctrine, advising that "we should become more conscious of the central role that command and control is likely to play in the future as a possible Achilles' heel of otherwise invulnerable systems" (Kahn 1960a, 301–302). The latter vulnerability was regarded as critical for the survival of the capacity to resist under nuclear attack and received increasing attention not only from Kahn but also from other researchers within the RAND Corporation.

Kahn's strategic planning focused on putting into place reliable systems of command and control that were guaranteed to survive and continue functioning after a nuclear first strike. The planning entailed putting in place "some kind of information gathering network of data-processing centers that can receive and evaluate information, make decisions and transmit orders, all in a matter of minutes and even seconds. It seems feasible to build systems that will do this even when under enemy attack" (Kahn 1960a, 187–188). The substitution of "feasible" for "desirable" is characteristic of Kahn and the RAND Corporation's can-do ethos—if it was necessary to invent such a network, then it had to be "feasible." The only limitation Kahn seemed to place on the network was that it be analog, adding that "Nobody is yet willing to trust the decision of war or peace to a computer" (Kahn 1960a, 188). However, this was precisely part of the pragmatic response of a key technical researcher in the RAND Corporation to Kahn's strategic call for a system of command and control able to continue functioning after a nuclear first strike.

Kahn and the RAND Corporation's strategic requirements for ensuring the survival of the United States' capacity to resist contributed to the thinking that helped lead to the invention of the Internet. This is well-known, and a common response to the view of the military, Clausewitzian origins of the Internet is to present it as an interesting coincidence with few implications for future developments. However, such a genealogy is important

for formulating strategic postures for resistance involving the Internet given that its origins were themselves part of a resistance strategy. The contributions of the RAND Corporation researcher Paul Baran are especially important in this respect. His work was dedicated to supplying the network capable of technically delivering Kahn's strategic demand for a survivable system of command and control. In a paper from 1960 prepared for the United States Air Force—*On a Distributed Command and Control System Configuration* (Baran 1960b)—Baran cites Kahn's 1960 RAND Corporation paper *The Nature and Feasibility of War and Deterrence* (Kahn 1960b) as motivation for his invention of a survivable command and control network.

Baran and Information War

Baran sought a control and command structure—or capacity to resist—that could survive a nuclear first strike. The option of bomb-proofing physical cables was explored but considered prohibitively expensive and unreliable. Baran focused instead on the idea of decentralized networks—first linking AM radio stations bearing only two messages—initiate and cease attack—then the telephone network, moving finally to theorize a distributed communication network with built-in redundancy and the ability to transmit discrete message packets. Baran later reflected:

> If the strategic weapons command and control systems could be more survivable, then the country's retaliatory capability could better allow it to withstand an attack and still function; a more stable position. But this was not a wholly feasible concept because long-distance communication networks at the time were extremely vulnerable and not able to survive attack. That was the issue. Here a most dangerous situation was created by a lack of a survivable communication system. That, in brief, was my interest in the challenge of building survivable networks. (Baran cited in Naughton 2000, 96)

In a series of RAND Corporation papers ranging from *Reliable Digital Communications Systems Using Unreliable Network Repeater Nodes* (Baran 1960a) in 1960 to *On Distributed Communications* (Baran 1964) in 1964, Baran proposed a distributed, decentralized network as the structure of communications most resistant to enemy attack. He also proposed that it be used to transmit bursts of digital information (later called "packets") that could arrive by any number of routes across the network to be re-assembled at the receiving station. This would ensure that the network would be neither fatally compromised nor overloaded in the event of an attack. Both the network structure and the digital modality served to enhance the system's capacity to resist.

While it is widely accepted that Baran's work indirectly provided the intellectual inspiration for the Internet, it is also held that its implications pointed beyond the military matrix in which it was conceived. It was an example of research of considerable civil import funded by the military but openly published and subject to scientific debate and public applications that far exceeded its contribution to defense (see Warnke 2011). However, as with everything published by the RAND Corporation, even the fact of publication was of strategic significance—and Baran's papers were no exception. The RAND Corporation was happy with the USSR knowing that the USA had theorized and was moving to implement a survivable control and command system. Indeed, the adversary's knowledge of the possibility and existence of such a system was essential to its working as effective deterrence. Even so, it might be argued, the implications of the research into distributed and thus decentralized networks eventually exceeded even this strategic context, providing the conditions for an emancipatory use or resistance of the non-hierarchical network.

Internet as Control

This view became a powerful ideological argument for an antihierarchical, even libertarian, view of the net that saw in its decentralized architecture an unanticipated possibility for non-hierarchical exchanges of information. Unfortunately, this view neglects other forms of control over the distribution of information that were also designed into the distributed network. We now know that debates within the RAND Corporation concerning distributed networks were accompanied by research into cryptography and the concealment of message paths and contents in a system with the potential to archive and make available to surveillance all of its communications. Baran's distributed network was also a cryptonomicon since a distributed network had an even greater need for cryptography, building secrecy and the control it afforded into its very architecture. This interest and the research it generated were secret and withheld from the published papers, which were consequently in no respect the unintended "free gift" from the military to a future non-hierarchical and democratic Internet.

The RAND Corporation's proposal foundered in the face of opposition from the telephone companies; however, Baran's papers were noted in the UK in the National Physical Laboratory (Donald Davies and packet-switched networks) and brought to the attention of another US strategic body—the Defence Advanced Research Projects Agency—known as ARPA (dropping the D). The detail of the history is complicated, but the same problem of a survivable network, decentralized but with compensating cryptography to ensure concealed control, persisted in the networks that evolved towards the Internet. In spite of their apparently non-hierarchical architecture, the history of these networks and their theoretical inspirations points to the construction of the Internet as an *arcanum* or space of secrecy.

How to Resist the Internet

This brief account of the concealed role secrecy played in the early formulations of the Internet puts into question any imprudent use of the Internet as part of a resistant strategy. It would not be an exaggeration to regard the Internet as one of the most prominent contemporary theaters for the struggle of contemporary resistance movements to invent, maintain, and enhance a radical capacity to resist. The struggle is conducted on two main fronts: the first is resistance to the state's claim to a monopoly of information and strategy and the second, resistance to state infiltration and surveillance of social networks and the capacity to resist they have helped bring into existence. The first front is the struggle for and against secrecy—the attempt to sustain powerful encryption on the web against the will of the state and also the effort to compromise state and corporate encryption. This struggle has a history dating back to the 1990s, in which Wikileaks, the Edward Snowden US National Security Agency (NSA) exposures, and Anonymous are but the most recent skirmishes. At stake is the state's claim to monopolize the information transmitted on the web and to archive its movements and content at its openly illegal pleasure. Ironically, Chelsea (Bradley) Manning and Snowden's whistleblowing was made possible by a relaxation of the rules of access to the *arcanum* that was part of the strategic response to 9/11 and the view that the USA's capacity to resist had been compromised by excessive secrecy and the reluctance of the intelligence agencies to share information. The redistribution of the *arcana* of state secrecy, which was thought strategically necessary to secure the capacity to resist a new kind of enemy, paradoxically undermined it by extending access and making its secrets vulnerable to public exposure.

The other side of the coin of exposing the *arcana* of state is maintaining oppositional or civil secrecy through encryption. This is a difficult and fallible project, but one which is pursued with great strategic clarity and a keen sense of the paradox involved

in protecting civil society (Öffentlichkeit) through secrecy. This is an old problem, going back to the publication of Immanuel Kant's essay "Answering the Question: What is Enlightenment" (Kant 1784) in the pages of the journal of a secret society—the *Berlinische Monatsschrift*. The strategic stakes involved, however, should not be underestimated, since such efforts on the part of civil society constitute a challenge to the emergent claim to a monopoly of secrecy on the part of the state.

The ability to compromise the state's capacity to resist by weakening its monopoly of secrecy and hence its strategy is an important complement to the ability to use social media in constituting an oppositional capacity to resist on the part of civil society. The two campaigns are usually understood separately, but compromising the state's ability to survey civil society's use of the Internet is essential for the latter's ability to resist the state. For this is one of the simultaneous strengths and weaknesses of using social media to foster strategic discussion and to organize resistance. They can certainly deliver unprecedented levels of articulated and disciplined mass action, but also every step in constituting the capacity to resist and mounting resistance—as in the Istanbul Taksim Republic for example—can be traced and policed if the resistance is not successful. The very arts that permitted the creation of a capacity to resist on the eve of resistance can also undo it on the day after. Megadata can be used to trace associations (routine work for the NSA and other intelligence agencies) and to reconstitute with extreme precision the oppositional capacity to resist and its key members—militants and theoreticians—and even to proceed to their physical elimination (see Chamayou 2015). From one point of view, the web can liberate resistance and create a new capacity to resist, but from another it can also serve as the instrument for its decisive repression.

New Capacities to Resist

Rosa Luxemburg's dictum that resistant struggle itself gives rise to new capacities and constituencies of opposition was vindicated by the resistant actions in Hong Kong. Haunted by the memory of the failure of the Tiananmen Square occupation in 1989, which compromised the Chinese population's capacity to resist for over a quarter of a century, demonstrators associated with the two main strands of the Hong Kong resistance—Occupy Central with Peace and Love and the student Scholarism movement—adopted a strategy that they hoped would ensure the survival of the capacity to resist in the prospect of what Mao himself described in the 1930s as a "protracted war of resistance." Alongside the restraint and commitment to non-violence shown by the resistants—by now classical resistance tactics learned from Gandhi and the US civil rights movement—were a number of effective tactical innovations. The most striking was the conscious effort to limit the use of social media for strategic and tactical discussion in order to avoid leaving a record of the constitution of a capacity to resist that would help the authorities to unravel and compromise it at a later date. The demonstrators made wide use of the app *FireChat*, which makes an off-grid social network possible using Bluetooth and Wi-Fi—ideal for mass gatherings. Over 100,000 copies of the app were downloaded in a day, putting the app to a use that doesn't seem to have been anticipated by its designers (they say on their website, perhaps with *faux naïveté*, "Whether you are on the beach or in the subway, at a big game or a trade show, camping in the wild, or even travelling abroad, simply fire up the app with a friend or two and find out who else is there"). The strategic benefit is nevertheless clear: one of the devices connected to FireChat can serve as a portal to the web and to exposed on-grid global social media; this device could employ deep encryption, and the decrypted messages then disseminated through FireChat in a way that left few traces for the state to follow later. This was an example of strategic prudence characteristic of both previous and contemporary resistant

politics; it complemented and further mobilized the resistant virtues of a non-negotiable passion for justice and courage. It testified not only to the need for resistance and protest, but also to prudence in the choice of means through which they are pursued, above all through what Clausewitz identified as the prime objective of a resistant politics—the creation and preservation not just of an act of resistance but more importantly of the capacity to resist.

Yet I should end with some comments on the desirability of a resistant intervention that frontally challenges the state's claimed monopolies of violence and secrecy. It brings with it a number of problems that might make us wary of adopting it too enthusiastically as a political philosophy or technique. First of all, the emphasis on strategy and enmity in the theory of resistance brings resistant politics too close to the model of warfare—perhaps politics and political reason are and should be distinct from strategy? In this case, the ever closer relationship between state monopolies of violence and secrecy might provoke disproportionately violent responses to any threat posed to its monopoly of secrecy and an escalation of conflict that can only compromise the capacity to resist. Furthermore, perhaps a resistant politics, however ingenious and imaginative its tactical innovations, is ultimately reactive, reacting against initiatives of its adversaries—as was the case in Hong Kong—and not initiating and guiding political change. Perhaps, too, resistance is too somber a politics, whose emphasis on the cardinal virtues of courage, prudence, and justice limits the emancipatory élan that is characteristic of revolutionary politics to questions of survival under conditions of repression and open attack. And finally, perhaps resistance is less a political philosophy than a politico-military technique, one that can be adopted in the name of emancipation but also in the name of reaction and repression. This leads to the final concern or question—if the *arcanum* is indeed an important site of current interventions and requires an appropriately encrypted resistant strategy, what implications

will this have for the existence of a public sphere and even democracy?

References

Assange, Julien, Jacob Appelbaum, Andy Muller-Maguhn, and Jeremie Zimmermann. 2012. *Cypherpunks: Freedom and the Future of the Internet*. New York/London: OR Books.

Baran, Paul. 1960a. *Reliable Digital Communications Systems Using Unreliable Network Repeater Nodes.* Santa Monica, CA: RAND Corporation. Accessed April 9, 2017. https://www.rand.org/pubs/papers/P1995.html.

Baran, Paul. 1960b. *On a Distributed Command and Control System Configuration*. Santa Monica, CA: RAND Corporation. Accessed April 9, 2017. https://www.rand.org/pubs/research_memoranda/RM2632.html.

Baran, Paul. 1964. *On Distributed Communications: I. Introduction to Distributed Communications Networks*. Santa Monica, CA: RAND Corporation. Accessed April 9, 2017. https://www.rand.org/pubs/research_memoranda/RM3420.html.

Chamayou, Gregoire. 2015. *Drone Theory.* London: Penguin Books.

Erskine, Ralph, and Michael Smith, eds. 2011. *The Bletchley Park Code-Breakers*. London: Biteback Publishing.

Kahn, Herman. 1960a. *On Thermonuclear War.* Princeton: Princeton University Press.

Kahn, Herman. 1960b. The Nature and Feasibility of War and Deterrence. Santa Monica, CA: RAND Corporation. Accessed April 9, 2017. https://www.rand.org/pubs/papers/P1888.html.

Kant, Immanuel. 1784. "Beantwortung der Frage: Was ist Aufklärung?" *Berlinerische Monatsschrift* 12: 481–494.

Naughton, John. 2000. *A Brief History of the Future: The Origins of the Internet*. London: Phoenix.

Stephenson, Neal. 1999. *Cryptonomicon*. London: Arrow Books.

von Clausewitz, Carl. 1832–1834. *Vom Kriege: Hinterlassenes Werk des Generals Carl von Clausewitz*, vols. 1–3. Edited by Marie von Clausewitz. Berlin: Ferdinand Dümmler.

Warnke, Martin. 2011. *Theorien des Internet*. Hamburg: Junius Verlag.