Research Article

Digital Security for a Nonviolent Defence System

Brian Martin[1]

1. Humanities and Social Inquiry, University of Wollongong, Australia

Most discussions of digital security assume a society's defence system is based on military forces. If defence were organised differently, this would change digital security considerations. One alternative model for defence is organised popular nonviolent resistance to deter aggression and defend communities. This is called social defence, nonviolent defence, civilian-based defence or defence by civil resistance. Proponents have developed many ideas about how such a defence system would operate, but most of this work predates the Internet. A key element of nonviolent defence is communication. Resisters need to be able to communicate reliably with each other as well as communicate with aggressors, actual and potential. A centralised communication system that can be taken over by force is a serious vulnerability, so network systems like the phone system are preferable to broadcast media like television. However, many network systems enable surveillance, so nonviolent resistance would require a capacity to disable surveillance capabilities. Workers would be trained in taking control of systems and, if necessary, disabling them in ways that cannot be restored by enemy experts or threats to key personnel. Citizens from every walk of life would be expected to learn about digital security measures, and to practise using them in the manner of fire drills. Digital systems suited for nonviolent resistance to foreign aggression are also suited for resistance to authoritarian governments. Therefore, social defence planning provides a template for the agenda of digital activism to support peace and a different paradigm of security.

Corresponding author: Brian Martin, bmartin@uow.edu.au

Introduction

Most of the world's major countries have military forces, and this affects their thinking about digital security. For example, much military planning is carried out in secret, and relevant information is guarded from potentially hostile eyes. Governments with nuclear weapons guard access to targeting and launch plans extremely carefully. Similarly, efforts are made, covertly, to acquire information about the capacities and plans of rival military powers, such as nuclear launch plans. The result is a type of digital information security race, analogous to the more well-known arms races. Rival governments want to protect their own information while acquiring information about their opponents, and sometimes their allies.

Such concerns would be radically reoriented by defence being organised in fundamentally different ways. For example, dozens of small countries do not have armies[1] and therefore do not require protection of their own military information. Some countries have made preparations for civil defence, which involves protection of the population and some infrastructure from foreign attack, for example in underground shelters. Civil defence can benefit from a digital component, to communicate after attack, that needs protection, but there is not the same urgency to protect such communication from external scrutiny.

Here I look at the implications of a model of defence based on nonviolent community resistance to aggression using methods such as rallies, marches, strikes, boycotts, fraternisation and sit-ins. It has several names: social defence, nonviolent defence, civilian defence, civilian-based defence and defence by civil resistance. Although no society has ever adopted a system of social defence, there are relevant historical examples and a body of writing sufficient to indicate its basic features. In particular, communication, and appropriate information and communication technologies, are crucial elements of a social defence system. Examining the implications of social defence for digital peace and security is useful in two ways: it provides insight for those who see social defence as a worthwhile alternative, and it illuminates assumptions underlying current policies on the digital realm.

In the next section, ideas about social defence are introduced. After this, the role of communication in social defence is examined in some detail. Finally, the implications of moving towards social defence are canvassed, along with insights about possible relevance to current policies. Given that social defence is a possible rather than an implemented alternative, the approach here draws on historical examples and general principles to map out broad-brush implications for digital security.

Social defence

There is a long history of people using nonviolent means to challenge repression and oppression. In the mid 1800s, Hungarians resisted their domination by the Austrian empire by, for example, refusing to speak German, refusing to serve in the Austrian army, boycotting Austrian businesses and refusing to pay taxes. Notably, they did not resort to armed resistance. After many years, the Hungarian campaign eventually succeeded[2]. Similarly, beginning in 1898, Finnish nationalists similarly resisted control by the Russian empire without using arms, their struggle succeeding in 1905[3]. These and other campaigns helped inspire Gandhi's campaigns against racial discrimination in South Africa and in the struggle for independence and self-reliance in India. Gandhi is the pioneering figure in the history of nonviolent action: he was the first to treat it as a strategic approach to social change.

The struggles of the Hungarians and others, and Gandhi's campaigns, inspired some thinkers to imagine that nonviolent methods could be used to replace military defence. The advent of nuclear weapons and the rivalry between the United States and the Soviet Union stimulated thinking about nuclear disarmament because there is no reason for a country without military forces to be a nuclear target. Complete disarmament is a logical extension; social defence is an alternative defence option. This option was developed by a variety of writers mainly from the 1950s onwards (e.g., Boserup & Mack[4]; Burrowes[5]; Drago[6]; Johansen & Martin[7]; King-Hall[8]; Niezing[9]; Sharp[10]). The rise of the massive movement against nuclear weapons in the 1980s helped stimulate interest in social defence. There were citizens groups promoting this option in Australia, Britain, France, Germany, Italy, Netherlands, Norway, Sweden and the US. Several governments sponsored investigations (e.g. de Valk & Niezing[11]), and the Swedish government included social defence as one component in its system of 'total defence,' which however was primarily military. However, after the end of the Cold War, and the apparently reduced risk of a major war in Europe, social defence fell off the agenda for both activists and governments.

A common assumption in military planning and everyday discourse is that superior force will always defeat an opponent. With this way of thinking, it seems that social defence is bound to fail in the face of a determined aggressor. However, research on nonviolent action, also called civil resistance, offers a different perspective. Chenoweth and Stephan[12], in a study of hundreds of campaigns against regimes or occupations or for secession found that nonviolent campaigns were more likely to succeed, and furthermore nonviolent regime changes were more likely to lead to freer societies years later. Chenoweth and Stephan also found that the success in nonviolent campaigns did not correlate with the level of repression of the opponent regime. In other words, nonviolent campaigns are just as successful against highly repressive regimes as against more tolerant ones.

The theory underlying nonviolent action and social defence is that systems of rule depend on the acquiescence and cooperation of most of the subjects[13]. If people withdraw their support for the ruler, the regime will collapse. Crucial here is recognising that police, troops and administrative functionaries are included: if they decide not to cooperate, then no ruler can maintain power.

Nonviolent resistance operates by undermining the willingness of opponents to maintain their aggressive activities. It is important for resisters to avoid using violence. Wider sections of the population, including women, children, the elderly and people with disabilities, can join nonviolent actions. Most soldiers are less willing to use force against civilians than against armed opponents. When they attack unarmed civilians, this can create a backlash, called political jiu-jitsu, generating more support for the resisters[13]. For example, when Indonesian troops opened fire on East Timorese people attending a funeral, and the massacre was witnessed by Western journalists, this generated much greater international support for East Timor's independence[14].

No society has adopted a full-scale social defence system, but nonetheless there are some suggestive historical examples. In 1923, French and Belgian troops occupied the Ruhr, a productive area in Germany, because the German government had fallen behind in its World-War-I reparation payments. Unable to resist militarily, the German government supported people in the Ruhr in a variety of methods of nonviolent resistance, for example refusing to operate trains. The resistance was an important factor in the invaders eventually withdrawing[15]. In 1968, half a million Soviet and other Warsaw Pact troops invaded and occupied Czechoslovakia to thwart the development of a freer form of socialism. The Czechoslovak military did not resist; instead, there was a spontaneous citizens nonviolent resistance involving protests, noncooperation and fraternisation. Although the active resistance lasted only a week, it took the Soviet leaders eight months to install a puppet government in Czechoslovakia, and the invasion undermined Communist parties around the world[16].

There are a number of examples of spontaneous nonviolent resistance to coups, including Germany 1920, Algeria 1961, the Soviet Union 1991 and South Korea 2024. It should be noted that in most countries around the world, military forces are more likely to be used to oppress the domestic population than to defend against foreign enemies. Social defence, by eliminating military forces, also eliminates the risk of a military coup.

Like military defence, social defence is not guaranteed to succeed. As with any form of defence, much depends on planning, training and investment. Every year, there is a vast expenditure on military preparations. It remains to be seen whether a similar effort on social defence could lead to equivalent benefits. Arguably, governments have little interest in the potential of social defence because introducing it would provide skills and training for members of the population that could be used against governments themselves. According to this way of thinking, social defence is dismissed not because it has low prospects of success but because it is a threat to vested interests.

Communication and security in social defence

In a social defence system, several types of communication are crucial[17]. Communication with opponents, such as invading or occupying troops, is vital for the purpose of dissuading them from their duties. Some of the Warsaw Pact soldiers who were part of the force invading Czechoslovakia in 1968 had been told they were there to prevent a capitalist takeover. When told by Czechoslovaks that they were socialists too, some of the troops became unreliable. It helped that Czechoslovaks had been taught Russian in school, so they could speak to Russian conscripts.

In military engagements, there is little direct communication between combatants on the opposing sides. In social defence, in contrast, it is crucial to facilitate this sort of communication, which implies studying foreign languages, cultures and ideologies. Technology becomes important when face-to-face contact is difficult. Part of a social defence communication strategy could involve creating connections with opponents through direct messaging, social media and broadcast media.

Communication among resisters is also important, to share information, maintain morale and coordinate tactics. In 1968, the Czechoslovak radio network played all these roles. When the Soviets brought in jamming equipment by train, this information was broadcast on the network and the train was shunted onto a siding. The network announced a meeting of the Czechoslovak Communist Party, which was united in opposition to the invasion; the meeting was held under the noses of the Soviet occupiers[18].

With the advent of the Internet, communication by various forms of online media is possible. It is now possible to organise rallies at short notice, without a lot of preparation, though in campaigns against governments this may sidestep valuable capacity building[19]. An analysis of violent attacks on unarmed protesters showed that when campaigners had built their own media capabilities, the attacks were more likely to trigger domestic mobilisation of resistance and defections by security personnel[20]. To counter online media, an aggressor might try to shut down the Internet, so a social defence system would necessarily need to implement several backup communication systems. In any case, shutting down the Internet has not been an effective way to stall popular mobilisations. When the Egyptian government closed the Internet in 2011 to stop the Arab Spring uprising, activists found various ways to work around the closure, and people not involved in the protests went to the streets to find out what was happening, and some of them joined the protests[21]. In building a social defence system, planners would learn from such experiences and seek ways to maintain communications in an emergency.

Similar considerations apply to vital facilities including food, water, energy, transport and medicine. For example, aggressors might try to subdue the population by closing down oil refineries and electricity-generating plants. Preparation for such eventualities could include designing the energy system around local self-reliance, such as local and community solar and wind power combined with energy efficiency. A large generating plant is a potential target for aggressors or terrorists; rooftop solar panels are not.

Communication systems can be used for surveillance[22][23][24]. An aggressor might try to obtain access to a network and use it to identify and track leaders of the resistance. There are several implications for planning a network. One concerns the role of secrecy: some nonviolent campaigners recommend being as open as possible about their plans, sometimes to the extent of inviting police to meetings. Following this line of thought, a social defence system could be transparent: its design could be made available for public scrutiny, for example describing planned responses to threats. Plans might well include scope for tactical innovation by local groups.

Another implication is the value of learning and sharing skills. Rather than relying on a few leaders for strategic planning and decision-making during struggles, resistance planning would include the development of strategic thinking and decision-making skills in a broad cross-section of the population. Therefore, if leaders were killed, arrested or coerced, others would be able to step into their roles. This sort of leadership in depth means that surveillance to discover leaders of the resistance would have limited benefit.

A third important role for communication is with third parties, those not directly involved in the struggle. When resisters are nonviolent, violent attacks on them can generate greater support: this is political jiu-jitsu. However, this greater support does not happen automatically: outsiders need to know about the attacks, hence the role of communication. Therefore, a priority in a social defence system is building secure communication links to outside groups, which might include like-minded groups in other parts of the world, mass and social media, and members of attacker groups.

A social defence system needs a capacity to understand threats, for example awareness of developments in potential aggressor states, the cultural and political dynamics in those states, and sources of opposition in those states. In essence, this is a sort of intelligence system, In the spirit of the participatory nature of social defence, its intelligence system could draw on a wide range of sources, including tourists, dissidents and personal connections via clubs and networks, such as in sports and cooking. The intelligence system could publish its assessments openly, thereby benefiting from feedback. This sort of 'publicly shared intelligence' was used, during the oil boycott of South Africa under apartheid, to track and expose vessels that attempted to sell oil to the government[25].

	Military defence	**Social defence**
Methods	Violent	Nonviolent
Participation	Soldiers (especially young fit men)	Citizens (men, women, children, elderly, people with disabilities)
Mechanism for victory	Superior force	Undermining the will of the opponent
Communication priorities	Within defence forces	Within community, with opponents and third parties
Decision-making process	Command system	Decentralised, cooperative
Digital security priorities	Protect own information, gather opponent's	Gather information about threats
Digital security participation	Intelligence agencies and leadership	Citizens

Table 1. Differences between military and social defence

Digital security in social defence

The primary goal of digital security in a social defence system is maintaining the capacity for reliable communication within the resistance, between the resistance and opponents, and with third parties, including those in other parts of the world, especially places from whence aggression might or does originate. This capacity needs to be maintained even if enemy troops have free access to every part of the community, and even if these troops use force to attempt to compel acquiescence. It needs to be maintained even if hostile operatives have access — potentially free access — to design principles and details of the implementation and operation of the communication and intelligence system of the defence.

There is an analogy with free software, which is open for inspection while still holding the capacity for reliable performance[26]. Free software often is more stable than proprietary alternatives precisely because the code is publicly available: interested parties can examine the code, point out flaws and weaknesses, and suggest improvements. This reduces the risk of bugs, intentional or otherwise. The keys here are open access and improvement based on participation by any interested party.

Similar considerations apply to setting up a digital infrastructure to support social defence. It is easier to spell out the principles underlying design and implementation than to give details of the result. The principles are resilience in the face of attack, and open and participatory design and maintenance. It is possible, nevertheless, to suggest some of what might be developed.

An obvious requirement is digital defence in depth: if primary systems are compromised, then back-up systems should be able to take over seamlessly. This is currently a design principal for military communications. For social defence, this principal needs to be applied to communication for the entire population, who are the defenders.

One obvious threat is shutting down the Internet and mobile communication networks. As noted, dictators have occasionally attempted to do this to quell mobilisation of resistance, but at the risk of stimulating greater opposition. For this reason, it makes sense for social defence communication systems to be co-located with civilian systems. Hence, any disruption of defence systems would immediately alert the entire population, and people elsewhere, about the threat.

A social defence system would be strengthened by strong connections with outsiders, especially sympathisers. At any given time, there could be numerous outsiders residing in the community, keeping in regular contact with outside networks, as well as numerous community members residing in other parts of the world. These connections could provide an early warning system about threats, including threats to communication channels.

Whatever communication system is established, it needs to be regularly tested. Military forces run training exercises, some of them full-scale, to ensure troops are prepared and systems are resilient. Likewise, in a social defence system it makes sense to run simulations of defending against attack; only one such simulation has ever been documented[27]. The simulations should be varied and designed to involve the entire population. They would be analogous to fire drills, except that they would require more initiative from participants and involve extensive post-drill evaluations.

Rather than specifying in advance details of the organisation of communication systems, it is easier to suggest the process by which these details would be developed, namely through participatory planning, regular testing, participatory evaluation, and revamping of systems as necessary.

Consider this detail as an illustration. In a computer system, normally an administrator controls access to passwords and other information that is not accessible by users. An aggressor might seek admin rights by threatening the admin or relatives with torture. The system could be set up so the admin can provide a dummy password that only gives access to innocuous information. Alternatively, in a crisis there could be an option to deny access to anyone unless they have an emergency password which would be held remotely. Another alternative would be for information that might be useful to an aggressor to be deleted in an emergency. The point of these options is to reduce the vulnerability to coercion: with options such as these, torture could not provide access; if potential aggressors know this in advance, they would have no justification to try.

Preparations along these lines could be made with widespread participation, so anyone interested would know how the system was configured. This applies also to hostile elements: it would be assumed that they too would know how the system was configured but, even with this knowledge, would have difficulty hacking it. This is analogous to public key encryption, in which the process of encryption is not secret but messages can be sent securely nevertheless.

It is possible to speculate about how digital systems would be organised for effective nonviolent defence against aggression, but this is hypothetical. Currently, large numbers of computer specialists have in-depth knowledge of programmes and systems. For the most part, the work of these specialists is geared to the priorities of governments and corporations. If even a relatively small number of them turned their skills to ensuring digital security for a nonviolent people's defence system, it is plausible to assume that simple yet sophisticated systems could be developed.

Transition considerations

While it is possible, on the basis of general principles, to spell out how a social defence system might be organised, much of the detail of implementation would be dependent on decisions made as the defence system was established, tested and evaluated. This presumes that such a transition process can occur in a straightforward manner. However, a more realistic assumption may be that governments will oppose moves towards social defence.

Another meaning of 'social defence' is defence against government repression and oppression. In this meaning, social defence involves a community defending itself against government and its functionaries, in particular the police and military. This sense of social defence speaks to the everyday reality that military forces around the world are seldom used to defend against attack by foreign militaries. More commonly, they are used to maintain control, sometimes in other countries — for example, the US military has a presence in over 100 countries, and numerous governments contributed troops to the war in Afghanistan — and especially of their own populations. In this way of thinking, armies serve primarily to maintain internal control, not to defend against external aggression.

From this perspective, social defence poses a fundamental threat to the government. A population with skills and preparation to defend against foreign aggression could turn those skills against the government itself. Therefore, the biggest challenge facing proponents of social defence is not providing a rational explanation for how it would work but in overcoming government indifference and hostility.

A transition strategy to social defence might involve efforts to develop skills and infrastructure that enable resilience in the face of aggression, and empower people to participate in resistance. By setting up systems that cannot be controlled or destroyed centrally, the population is less vulnerable. Therefore, current efforts towards local food cultivation, local renewable energy systems, and town planning around walking and cycling contribute to the sort of resilience needed in a social defence system. The point here is that there are common interests between movements for local self-reliance and the goal of building a social defence capacity.

The same ideas apply in the digital domain. Currently there are digital rights movements that promote systems and practices that preserve privacy and thwart surveillance. These movements favour secure encryption, promote the use of the Tor browser and the Duckduckgo search engine. They are critical of proprietary platforms like those provided by Facebook, Google and Amazon, which gather vast amounts of personal information that can be accessed by spy agencies. The orientations of digital rights organisations mesh with the sorts of digital systems likely to be used in a social defence system. The basic idea is that no aggressor could gain access to information unless it was purposely made public.

Consider Facebook for example, widely used by activists as well as many others. Relying on Facebook is a potential vulnerability given that an aggressor might be able to coerce access to Facebook data or to force shutting down of access to targeted groups. Those who promote less vulnerable alternatives to Facebook are helping build the sort of digital resilience needed for social defence.

This connection between current movements and social defence can be looked at in a different way: considering the sorts of digital systems that would best support social defence provides a direction for current digital rights campaigns. In many countries around the world, governments spy on their own citizens, often as a means of tracking dissidents and thwarting citizen movements. Digital rights movements are opposed to such surveillance and repression but are less united as to what alternative system should be the goal. Social defence provides a goal: increasing the capacity of a community to defend against aggression nonviolently. This implies, in accordance with typical digital rights demands, security against government and corporate surveillance. It also implies that systems for digital communications and storage be designed and operated in a participatory fashion. Of course there is a huge divergence between current systems, managed by the governments and corporations to protect their interests, and a system controlled and managed by citizen defenders.

Conclusion

Social defence represents a striking contrast to military defence. Most of the implications of social defence as a goal can be derived from two features: defence against aggression is carried out without the use of violence, and the defence system is based on popular participation rather than relying on professionals.

The implications for digital systems are also straightforward, though only in a general way. Unlike guns and explosives, digital systems on their own are not physically violent. However, digital systems can serve as tools to facilitate violence, for example to collect data to enable drone strikes. Digital infrastructure for social defence would be designed to minimise the potential for assistance in violence, given that aggressors might attempt to use coercion or guile to take over systems. In parallel, digital infrastructure for social defence would be designed to maximise the potential for nonviolent resistance, by enabling secure communication among resisters, with opponents and with third parties. How this would look remains to be seen, given that no community has ever been systematically organised for social defence. Nevertheless, the goal of building the capacity for social defence provides an agenda for campaigning today.

About the Author

Brian Martin is emeritus professor of social sciences at the University of Wollongong, Australia. He is the author of 23 books and hundreds of articles on nonviolence, scientific controversies, dissent, tactics against injustice, and other topics.

References

1. ^*Barbey C. Non-militarisation: Countries without armies. Åland Islands Peace Institute. 2015.*
2. ^*Csapody T, Weber T. Hungarian nonviolent resistance against Austria and its place in the history of nonviolence. Peace & Change. 32(4): 499–519. doi:10.1111/j.1468-0130.2007.00464.x.*
3. ^*Huxley SD. Constitutionalist insurgency in Finland: Finnish 'passive resistance' against Russification as a case of nonmilitary struggle in the European resistance tradition. Finnish Historical Society. 1990.*
4. ^*Boserup A, Mack A. War without weapons: Non-violence in national defence. Frances Pinter. 1974.*
5. ^*Burrowes RJ. The strategy of nonviolent defense: A Gandhian approach. State University of New York Press. 1996.*
6. ^*Drago A. Difesa popolare nonviolenta: Premesse teoriche, principi politici e nuovi scenari. EGA. 2006.*
7. ^*Johansen J, Martin B. Social defence. Irene Publishing. 2019.*
8. ^*King-Hall S. Defence in the nuclear age. Victor Gollancz. 1958.*
9. ^*Niezing J. Sociale verdediging als logisch alternatief: Van utopie naar optie. Van Gorcum. 1987.*
10. ^*Sharp G, Jenkins B. Civilian-based defense: A post-military weapons system. Princeton University Press. 1990.*
11. ^*de Valk G, Niezing J. Research on civilian-based defence. SISWO. 1993.*

12. ^*Chenoweth E, Stephan MJ. Why civil resistance works: The strategic logic of nonviolent conflict. Columbia University Press. 2011.*
13. a, b*Sharp G. The politics of nonviolent action. Porter Sargent. 1973.*
14. ^*Kohen AS. From the place of the dead: The epic struggles of Bishop Belo of East Timor. St. Martin's Press. 1999.*
15. ^*Sternstein W. The Ruhrkampf of 1923: economic problems of civilian defence. In: Roberts A, editor. The strategy of civilian defence: Non-violent resistance to aggression. Faber and Faber; 1967. p. 106–135.*
16. ^*Windsor P, Roberts A. Czechoslovakia 1968: Reform, repression and resistance. Chatto and Windus. 1969.*
17. ^*Martin B. Technology for nonviolent struggle. War Resisters' International. 2001.*
18. ^*Hutchinson RD. Czechoslovakia 1968: The radio and the resistance. Institute for Peace and Conflict Research. 1969.*
19. ^*Tufekci Z. Twitter and tear gas: The power and fragility of networked protest. Yale University Press. 2017.*
20. ^*Sutton J, Butcher CR, Svensson I. Explaining political jiu-jitsu: Institution-building and the outcomes of regime violence against unarmed protests. Journal of Peace Research. 51(5): 559–573. doi:10.1177/0022343314531004.*
21. ^*Ghonim W. Revolution 2.0. Fourth Estate. 2012.*
22. ^*Landau S. Listening in: Cybersecurity in an insecure age. Yale University Press. 2017.*
23. ^*Schneier B. Data and Goliath: The hidden battles to collect your data and control your world. Norton. 2015.*
24. ^*Véliz C. Privacy is power: Why and how you should take back control of your data. Bantam Press. 2020.*
25. ^*de Valk G, Martin B. Publicly shared intelligence. First Monday: Peer-reviewed Journal on the Internet. 11(9). https://firstmonday.org/ojs/index.php/fm/article/view/1397/1315.*
26. ^*Weber S. The success of open source. Harvard University Press. 2004.*
27. ^*Olson T, Christiansen G. The Grindstone experiment: Thirty-one hours. Canadian Friends Service Committee. 1966.*

Declarations

Funding: No specific funding was received for this work.

Potential competing interests: No potential competing interests to declare.