The Ellul Forum

For the Critique of Technological Civilization

Violence, Terrorism, & Technology

Issue 32 Fall 2003

International Jacques Ellul Society
Berkeley, California, USA
www.ellul.org

Jacques Ellul at age 70. Photo by Lucia Gill, July 1982

"Liberating violence cannot establish a society's values; for if they are to be communal values they will have to be accepted as good and true by every member of the community (not only by a majority).

But that can never happen when the values are imposed by, or as the result of, violence. . . The Algerian war certainly has not led the Algerians to accept Western values."

Jacques Ellul
Violence, 1969, pp. 114-115

The Ellul Forum

For the Critique of Technological Civilization

Founded 1988

The Ellul Forum is published twice per year, in the Spring and Fall. Its purpose is to analyze and apply Jacques Ellul's thought to our technological civilization and carry forward both his sociological and theological analyses in new directions.

Editor
Clifford G. Christians, Univ. of Illinois, Urbana
Associate Editor
David W. Gill, Berkeley, California

Contributing Editors
Patrick Chastenet, University of Poitiers, France
Dan Clendenin, Stanford, California
Peter F. W. Davies, Buckinghamshire College, UK
Marva Dawn, Vancouver, Washington
Darrell J. Fasching, University of South Florida
Andrew Goddard, Oxford University, UK
Joyce Hanks, Univ. of Scranton, Pennsylvania
David Lovekin, Hastings College, Nebraska
Carl Mitcham, Colorado School of Mines
Pieter Tijmes, University of Twente, Netherlands
Gabriel Vahanian, Strasbourg University, France
Willem Vanderburg, Univ. of Toronto, Canada

Publisher
The International Jacques Ellul Society
www.ellul.org Tel/Fax: 510-653-3334
P.O.Box 5365, Berkeley CA 94705 USA

Dues, Subscriptions, & Payment Options
The Ellul Forum is sent twice per year to all members of the IJES or its francophone sister society, the AIJE. An annual membership/ subscription, anywhere in the world, costs US $20. Please send check or money order (e.g., international postal money order) *drawn in US funds* for $20 to "IJES", P.O.Box 5365, Berkeley CA 94705 USA---*or* make payment to "IJES" electronically at www.paypal.com. Be sure to note your address and the purpose of your payment.

Change of Address
Please notify IJES of any change in your address. Our mailings are infrequent and postal forwarding orders expire.

Manuscript Submissions
For *Ellul Forum* writers' guidelines, visit www.ellul.org---or e-mail: Editor@ellul.org---or write Cliff Christians, EF Editor, Institute of Communications Research, University of Illinois, 810 S. Wright St., # 228, Urbana IL 61801 USA We welcome your proposals.

Books, Reviews, News
Send books for review, book reviews, and news to David Gill, EF Assoc. Editor, P.O. Box 5365, Berkeley CA 94705. E-mail: IJES@ellul.org

Back Issues
Visit www.ellul.org for a complete index of back issues. Issues #1-30 are available (only) as a complete collection on a compact disc for US $15. Issues #31 onward are available for $5 per copy.

From the Editor

Jacques Ellul understood violence personally and came to grips with it intellectually. He lived in the maelstrom of war and violence. During World War II years, 1939-45, he was fired from his position on the Strasbourg University faculty (1940), his father was imprisoned and died under German military detention (1942), and Ellul and his family subsisted as refugee farmers while working with the Resistance in the Entre-deux-Mers region outside Bourdeaux. The rancorous debates over the Algerian fight for independence from France during the Fifties, the student revolts of the Sixties, and the ongoing street-level conflicts of juvenile delinquents and gang members were among Ellul's special concerns after the War.

Ellul's *Violence: Reflections from a Christian Perspective* (1970 English; 1972 French *Contre les violents*) is a provocative analysis not confined to war in a narrow sense but ranging broadly across the spectrum from coercive political acts to revolutionary violence to institutional violence. Mennonite Professor Mark Baker "re-views" this classic on page 20.

In his major analysis of Ellul's work on violence, Andrew Goddard observes that it is "structured around the poles of freedom and necessity" (*Living the Word*, *Resisting the World*, Paternoster, 2002, p. 197). Certainly it is natural that *The Ellul Forum* dedicated to "carrying forward Ellul's analyses in new directions" would publish this issue on violence and terror, and do so in broader terms than war itself. From the myriad problems in this violent 21st century, we focus on three—war, terrorism, and surveillance.

In this issue, Andrew Goddard examines Ellul's refusal of just war theory, despite its dominance in the Christian tradition. As a Professor of the History and Sociology of Institutions in the Law Faculty, Ellul would have appreciated Dal Yong Jin's historical and legal analysis of the technology of cyberterrorism. David Lyon is the research director of the international Surveillance Project based at Queen's University, investigating surveillance, risk management, and social ordering in global information societies. He reflects on the rapid growth in existing surveillance trends produced by 9/11.

The Ellul Forum nurtures networks of discussion and learning. Interested readers are invited to engage the authors directly (contact info given at head of each major article). As always, manuscripts (or proposals) you wish to have considered for *The Ellul Forum* are welcomed by the Editor. Material for "News and Notes," "Ellul Resources," and queries about book reviews should be sent to the Associate Editor, David Gill.

Our upcoming Spring 2004 issue (#33), guest edited by Joyce Hanks, will mark the tenth anniversary of Jacques Ellul's death.

+ + + + + + +

Mea culpa: our last issue (Spring 2003, #31) mistakenly omitted the name of Andoni Alonso from the title line as co-author (with Carl Mitcham) of the Ivan Illich obituary we republished from the Madrid daily *El Pais*. Our apologies to Andoni Alonso.

Clifford G. Christians, Editor ***editor@ellul.org***

Ellul On Violence and Just War

by Andrew Goddard

Andrew Goddard (andrew.goddard@ wycliffe-hall.oxford.ac.uk) is Tutor in Christian Ethics at Wycliffe Hall and a member of the Theology Faculty at Oxford University. His new book Living the Word, Resisting the World: The Life and Thought of Jacques Ellul *(Paternoster, 2002) is reviewed on page 19 of this issue of* The Ellul Forum.

How should Christians respond to the violence of war ? What are those, who want to be faithful disciples of Christ, to say and to do? As Ellul states in the opening sentence of his book on the subject, "The churches and theologians…have never been in unanimous agreement in their views on violence in human society".[1] There has, nevertheless, been a predominant approach to the question of war, namely that of the "just war tradition". Ellul is a trenchant critic of this way of thinking and yet, as often in his writing, his comments are lacking in detailed engagement with the specific arguments of his opponents. Instead, he provides a broad-brush account and critique. While making some strong and valid objections, this is bound to leave anyone sympathetic to the just war tradition feeling rather dis-satisfied, perhaps even that they have been subjected to the "violence" of caricature.[2]

Given the importance of this subject and the strong differences of opinion found among Christians which results in divided witness to the world, it is necessary to step back and identify the fundamental differences between the just war tradition and Ellul's thinking and to ascertain whether any constructive dialogue can take place between them. This article highlights two areas in which the wider rationale and method of Ellul and the just war tradition stand in tension with each other, and it acknowledges both strengths and weaknesses that can be seen when the two approaches are placed in dialogue.

The heart of the divergence between Ellul's account of violence and that of the mainstream Christian tradition is perhaps most easily understood by reference to the two terms which identify that tradition – "just war". Ellul questions both the central moral category and frame of reference to be used in thinking about the subject and the central moral task of such moral thinking.

Subject Matter – War or Violence?

It is of the utmost importance that Ellul's account is focused on *violence,* and interestingly, in the original French is entitled *Contre les violents*.[3] The specific question of *war* is therefore set in the wider context of the phenomenon of *violence*. He does not concentrate on "hostile contention by means of armed forces, carried on between nations, states, or rulers, or between parties in the same nation or state; the employment of armed forces against a foreign power, or against an opposing party in the state."[4] Instead, he insists that thinking about this specific subject can only be properly done once there is, in the words of the title of his book's third chapter, "Christian realism in the face of violence".

This approach marks a significant shift in understanding the question. The great Christian theologians of the just war tradition generally approach their discussion from two angles. In some contexts, it is a question about how a confessing Christian with a particular political or military responsibility in society is to act or indeed whether they can faithfully remain in certain positions given the duties that will be incumbent upon them.[5] In others, it is seeking to elucidate the obligations of love and the prohibitions entailed by the specific commandment against murder.[6] In thinking about "war", in other words, we are being asked to reflect on a form of practical, political action that raises a fundamental moral question because it requires participants to be involved in the taking of human life.

Ellul, from the opening pages of his book, resets and critiques this tradition within his own predominant category of violence. So, categorizing this strand of Christian thinking as "compromise", he places the early Christian concerns about the state in relation to "violence". "They saw that the state…used violence against its enemies, internal or external. For war certainly seemed violence pure and simple, and the police operated by violence" (p. 2). The challenge that remained even when Christians held political office and the state ceased persecution of the church is expressed in the following terms – "the political power…continued to use violence" (p. 3). Ellul then explains how theologians and canonists responded to this challenge of what he insists on calling "internal violence" and "external violence" by the state.

In relation to "internal violence" Ellul discerns two key redefinitions taking place. A distinction is drawn between the state and human beings, and it is held that the state "never acts by violence when it constrains, condemns and kills" (p. 3). Instead, its actions are distinguished from "violence" by being conceived of as "force" so that the state "is the institution which demonstrates the difference between violence and force…There is all the difference between violence and force" (p. 4). The issue then becomes whether or not the state's use of force is "just" or "unjust" and conformity to the law is here the determinative factor. However, even when the state does not conform to the law it still uses force – albeit now unjust force – rather than violence. This reasoning, Ellul claims, was an attempt "to clear the state of the charge of violence by explaining that it was not violence" (p. 5).

In relation to the external violence of war, Ellul contends that the church reasoned this way: "To deny the state the right to go to war was to condemn it to extinction;" yet the state was ordained by God, and therefore the state "must have the right to wage war" (p. 5). This he claims (though without citing any supporting evidence) was the origin and fundamental rationale for "the casuistry of the just war" whose evolving tradition he sums up in terms of seven conditions to make a war just. Although Ellul acknowledges that these "have theoretical solidity" (p. 6), he questions their practicality and relevance, especially in the contemporary world.

Ellul's own contrasting approach to the question is shaped by what he calls "Christian realism." "The Christian who wants to find out what he ought to do, must be realistic; this is the first step". The problem is that we need first to be clear what the Christian must be realistic about and herein lies the fundamental weakness of Ellul's work. "Violence" we have seen to be the lens through which he re-interprets and critiques the just war tradition. It is the phenomenon about which he insists we must be realistic. But "violence" is itself never defined by Ellul.[7] Clearly it is broader than the just war tradition's focus on the taking of human life, but just how broad it is remains unclear. The signs are, however, that for Ellul the term is exceedingly wide-ranging in its scope – "economic relations, class relations, are relations of violence, nothing else" (p. 86), "psychological violence…is simply violence, whether it takes the form of propaganda, biased reports, meetings of secret societies that inflate the egos of their members, brainwashing or intellectual terrorism" (p. 97). It would appear that Konyndyk is broadly correct that violent behaviour for Ellul is "coercing someone in a way that violates his personhood".[8] Given that "violence" is to be the over-arching interpretive category for Christian reflection on war, and is being used to explain Christian moral assessments in history which did not themselves primarily use this category, it would help if such a definition – or preferably a more precise one - had been given by Ellul himself.

Despite this weakness, there are two great strengths in Ellul's approach. Firstly, it refuses to mask the fact that punitive measures taken by political authority have the same basic structure as the wrong actions to which they respond. So fines (like stealing) take away people's property without their consent, imprisonment (like kidnapping) deprives persons of their liberty. Although this should be more obvious in war, the language of "force" means that it can be effectively forgotten. As Glover comments, "It is widely held that killing in war is quite different. It is not, and we need to think about the implications of this".[9] But this similarity need not mean moral differentiation is impossible: materially the act of sexual intercourse has a common structure whether it is joyful marital sex, adultery, fornication or rape; the insertion of a knife into human flesh could be an act of surgery or grievous bodily harm. Ellul formulates a stark law of the identity or sameness of all violence. When it is given a moral focus in order to insist that we cannot distinguish between just and unjust violence or violence that liberates and violence that enslaves, this simply asserts what really needs to be argued for.

Secondly, Ellul also highlights the continuity between the internal coercive actions of political authority ("police functions" as we might call them) and the external actions (military functions in war). Here there is continuity with the traditional just war understanding. That tradition similarly refuses to treat these as two independent spheres with different moralities or criteria for action. Ellul thus will be sympathetic to a common critique made by just war theorists. They point out that there is a tension (if not incoherence) in being a principled advocate of non-violent pacifism but not being a non-violent anarchist (Ellul's own position) or being committed to just war thinking but absolutely opposed in all circumstances to capital punishment. Where Ellul differs fundamentally is that the just war tradition is marked by seeing the task of political authority as one which can legitimately be fulfilled – at home and abroad, through police and through military – through the subordination of all uses of "violence" to the pursuit of justice.

Ellul himself held such views in his first published book where, in discussing biblical texts such as Romans 13 on the "use of the sword", he writes,

> The use of the sword in itself is not condemned…The use is subject to eventual condemnation…which will become a reality only if the sword…serves either the obstruction of justice or the spirit of power. Within this eschatological perspective, man's judgment in the realm of law assumes its rightful value. His judgment is the reason why the use of the sword will not be condemned. Any use of it apart from man's judgment runs counter to God's will….It is law which, before God, permits the use of force.[10]

Although it is difficult to be clear as to why Ellul departed from this viewpoint, one factor is perhaps found in his comment that the just war tradition is "based on the conviction that man can retain control of violence, that violence can be kept in the service of order and justice and even of peace" (pp. 5-6). Ellul's realism about violence appears to have led him to reject this fundamental presupposition which is essential to just war thinking. In contrast to the just war tradition and his own early views, not only does he place all reflection about war under the broader rubric and laws of violence, he sees violence (and so war as a subset within that) as a force which rules human beings. Occasionally in this writing he relates this to his theological understanding of the principalities and powers by naming violence as "one of the 'rudiments' (*stoicheia*) of this world".[11] This is, once again, a feature of Ellul's work which frustratingly he does not develop but it stands as a further reminder that the just war tradition, in making judgments about war, must avoid an unrealistic picture of sovereign individuals abstracted from the reality of power making choices about their actions. In making moral judgments about particular actions it is also vitally important to consider in all our thinking the work of the powers in the wider shaping of our society and politics.

The Purpose – Justification or Confession?

Ellul's differences with the just war tradition are not limited to his insistence on approaching the subject of war through the much larger category of violence then understood by him in a much more globalistic and quasi-deterministic fashion. He has a fundamental objection to just war's attempt to provide justification for certain violent actions. This objection would appear to take two forms.

First, in his realistic analysis of violence, one of the features Ellul identifies – his fifth and final law of violence - is that "the man who uses violence always tries to justify both it and himself" (p. 103). The horror and agony caused by violence means, he claims, that everyone who uses it seeks to demonstrate that they have acted morally when they have turned to violence. More controversial still – especially given that the Augustinian strand of the just war tradition appeals to "love of neighbor" as its rationale for the use of coercive force – Ellul explains that this universality of justification derives from the fact that "violence is an expression of hatred, has its source in hatred and signifies hatred….It is absolutely essential for us to realize that there is an unbreakable link between violence and hatred" (p. 104). The just war tradition is, therefore, in Ellul's eyes simply one of the multiple forms of self-justification inevitably developed by fallen human beings in the face of their own violence.

Second, although Ellul can apparently accept that Christians will use violence, he refuses to accept their justifications for this. Instead, he emphasizes that "as Christians we must firmly refuse to accept whatever justifications are advanced" (p. 140). He is insistent that "in their radical refusal to justify violence, Christians must not leave the smallest breach" (p. 141). Although particularly clear in his discussion of violence, this reflects a wider feature of Ellul's approach to the task of Christian ethics. He is constantly on the alert to prevent a Christian ethic from becoming a means of human self-justification that escapes God's gracious gift of justification by faith in Christ.[12] Violence, Ellul argues, is a sign of the fact that we have sinned and ruptured our communion with God. We must not, therefore, formulate means to justify it in certain circumstances. Instead, we must confess our sin and seek God's forgiveness. For Ellul, the important truth is that the Christian cannot have a good conscience. "The Christian, even when he permits himself to use violence in what he considers the best of causes, cannot either feel or say that he is justified; he can only confess that he is a sinner, submit to God's judgment, and hope for God's grace and forgiveness" (p. 138). It is, however, important to realize that Ellul as emphatically rejects pacifist-inspired forms of self-justification which are developed for a policy of non-violence. He is quite honest that, "in the face of the tragic problem of violence, the first truth to be discerned is that, whatever side he takes, the Christian can never have an easy conscience and never feel that he is pursuing the way of truth" (p. 138). Yoder is therefore right to describe Ellul as holding the view that "the Christian will have to use violence but will know that it is sinful",[13] but Ronald Ray is also correct in drawing attention to the fact that "even the Christian position of non-violence involves guilt".[14]

This approach to the question of a Christian attitude to war provides a necessary challenge to some of the uses Christians make of the just war tradition. That tradition too easily becomes a means by which "our side" in a military conflict is able to claim moral superiority over the enemy and believe itself not guilty. Too many politicians and Christian leaders uncritically apply the "criteria" for a just war in a simplistic manner. They can simply become a checklist of tests in order to show that the decision to go to war is justified and that right is on the side of their government. Ellul, in contrast, highlights the painful and tragic reality of living in a fallen world and being, in Luther's famous phrase, *simul justus et peccator*.

There is, however, a major weakness in Ellul's approach. This is found in the fact that in its aversion to any form of self-justification it is of little or no practical help to people faced with the harsh realities of living and acting in the real world. Two pieces of evidence show the dangers in Ellul's approach. Firstly, he appears incoherent and inconsistent when he attempts to make moral distinctions between different violent acts. He will state that as a Christian he "cannot call violence good, legitimate and just" (p. 133) and yet there are situations when he says he approves of certain violent acts (p. 69). Indeed, in the original French, he even writes of conditions in which the use of violence is acceptable and not condemnable.[15] Yet later he can write that violence is always condemnable.[16] [17]

Secondly, when it comes to the full and extreme horrors of war, we see the further difficulty in treating all violence as the same and refusing to offer any means of moral discrimination. Here, Ellul appears to accept that "anything goes" once war has begun and to refuse any moral constraint lest those who accept the proposed limits then believe they are justified in the limited violence that they do use. So, in conversation with Patrick Troude-Chastenet he reflected on the French experience in Algeria in these terms:

> According to me, once you have decided to go to war you have to go all out and use every means at your disposal. This is the case that applied in Algeria. Everyone was shouting their heads off

> against the torture that was going on. But the real problem was not the torture but the war itself. There is no morality in war. If you want to win you must pull out all the stops.[17]

Ellul is thus in a paradoxical situation compared to the just war tradition. That tradition seeks to limit war by acknowledging certain carefully delineated situations in which the use of coercion is justified. In so doing, it also lays down clear boundaries and a duty in certain contexts to sue for peace rather than to use immoral means. Ellul, in contrast, stands resolutely opposed to violence. However, his refusal to distinguish between different forms and levels of violence, his rejection of anything that could be construed as justification for violence, and his emphasis instead on the need to confess our necessary sinfulness in the fallen world, means that Christians guided by his approach may find themselves ending up involved in torture as a sad necessity (or presumably dropping nuclear weapons) in military conflict.

In short, Ellul has an aversion to any approach to moral thinking that he believes risks facilitating self-justification or denying the continuing presence of sin in all our actions. Pushed to an extreme, however, this makes his writing incapable of providing moral guidance or setting clear and realistic moral limits. As Oliver O'Donovan comments in his discussion of whether killing is a moral evil that we are bound at all costs to avoid and thus participation in war totally prohibited,

> The curious hybrid notions of "sin within the realm of necessity"(J.Ellul) and "responsible assumption of guilt" (H. Thielicke) capture dramatically the subjective moral tension which belongs to a decision of such gravity, but they leave the deliberative question in paradox and so seem to have more rhetorical than conceptual persuasiveness.[18]

Perhaps nothing illustrates the difficulty more sharply than Ellul's startling claim that "apart from the inspiration of the Holy Spirit, the use of violence is always an *a priori* contrary to the will of God".[19] How one discerns the Spirit's inspiration to use violence is, sadly, unelaborated. Presumably to attempt to do so would be to deny divine freedom and risk providing a means of self-justification!

Conclusion

Ellul and the just war tradition clearly approach the subject of moral judgment in war from quite different perspectives. It is important to recognize that these different approaches to the subject then shape their different conclusions.

In the light of the valid criticisms and cautions raised by Ellul but also the serious weaknesses in his own method, the challenge is whether or not a third way is possible. This could represent a chastened form of just war thinking in the light of Ellul's critique. In contrast to Ellul's work (where his attempt to reconfigure the Christian tradition by making "violence" the controlling concept risks distorting the structure of the tradition's account of morality in war) this would recognize and build upon the strengths of the just war tradition. Rather than just subsuming war under a strong account of "violence" and eschewing anything that could amount to self-justification, this would provide a careful structured analysis of the key questions which must be addressed in thinking about going to war and conducting war: who is to wage war? why should they have recourse to war? when should they do so? how should they fight? It would draw on the wisdom of the just war tradition to discern where significant moral boundaries lie in each of these areas.

In particular, like Ellul in his earlier writing, it would be based on the conviction that the structure and limits which must be placed on any use of destructive or lethal force are defined by the fact that just judgment is not only necessary but good and the divinely ordained task of government in a fallen world. It is therefore certainly true that "violence" is a sign of the fallenness of the world – Ellul's emphasis on this must not be ignored even if it needs to be tempered – but it does not follow that all recourse to violence is the same and so moral discrimination impossible.[20] There is, for example, a difference between war in order to right wrongs (just cause) and war for self-aggrandisement even if the latter is sometimes masked behind a claim that it is the former. There is a difference as well as a similarity between attacking opposing armed forces and engaging in torture of prisoners of war or blanket bombing of non-combatants.

This approach would, however, need to remedy the weaknesses in the just war tradition that become evident in the light of Ellul's approach. In particular it must redress the tendency to be unrealistic about the nature of human violence. There has to be a challenge to the idealism about human control in the face of the power of violence that so often undermines just war thinking. Perhaps most important of all, Ellul's critique has highlighted the tendency of the just war pattern of thinking to be hijacked for self-justification which masks the pervasiveness of human sin. The tradition could, however, be used as a more critical and prophetic tool. It would then raise before those holding political power and claiming to act justly, the challenging questions of their own complicity in global injustice and their enthrallment to the powers of Technique and propaganda as they make decisions about war in the contemporary world.

As in so many spheres of his thought, Ellul's work on violence runs the risk of an "all or nothing" response. Those attracted to the just war tradition easily ignore him as of no relevance to the realities of international power politics. Those eager for a prophetic Christian voice easily buy uncritically into his sweeping analysis of violence and by dismissing the tradition as "casuistry" and "compromise" find they are unable to offer guidance to those – including many Christians - with the terrible responsibilities of political authority. By recognizing the deeper divergences in method and focus between Ellul and the just war tradition and outlining both his strengths and weaknesses, it is possible to go beyond Ellul's work and develop a realistic analysis of the nature of war today that draws on the majority Christian tradition Ellul himself once embraced in order to encourage a prophetic yet discriminating voice for those seeking to be faithful disciples of Christ.[21]

References

[1] Jacques Ellul, *Violence: Reflections from a Christian Perspective* (London : SCM Press, 1970), p. 1. All page references in the text refer to this volume.

[2] The main critiques and account of the historical origins of the tradition are found in his categorisation of this approach as one of "compromise" (*Violence*, pp. 1-9) and his appendix on conscientious objection (*Anarchy and Christianity*, Grand Rapids: Eerdmans, 1991, pp. 91-5). A less polemical account of the origins of the Christian just war tradition is found in his study of the history of institutions (*Histoire des Institutions Vol 2*, (Paris: PUF, 1989, pp. 506-7, 525-7). Particularly given our current context, it is also important to note that he sees this tradition in part shaped by Islam's subversion of Christian faith (*Subversion of Christianity*, Grand Rapids: Eerdmans, 1986), pp.100-4.

[3] Jacques Ellul, *Contre les violents* (Le Centurion, 1972).

[4] Oxford English Dictionary's primary definition of 'war'.

[5] So, in the tradition, among the key classic texts are Augustine's letter to Count Boniface (Letter 189, from 418AD) with the counsel, "Do not think that it is impossible for any one to please God while engaged in active military service" and Luther's "Whether Soldiers, too, Can be Saved" (1526) written to respond to the concerns of Assa von Kram of Wittenberg about reconciling his Christian faith and military profession.

[6] Thus Aquinas' main discussions in the *Summa* are (a) *ST* II-II, q40 which is entitled "of war" and, importantly, under the discussion of charity and (b) *ST II-II*, q64 "Of Murder".

[7] This is a common criticism of Ellul's writing; for example, "The first question, then would seem to be: What is violence? But, strangely, Ellul does not address it" (Kenneth J. Konyndyk, "Violence" in Clifford G. Christians & Jay M. Van Hook (eds), *Jacques Ellul: Interpretive Essays* (University of Illinois Press, 1981), p. 256.

[8] Konyndyk, *op.cit.*, p. 256.

[9] Jonathan Glover, *Causing Death and Saving Lives* (London: Penguin Books, 1977), p. 251.

[10] Jacques Ellul, *The Theological Foundation of Law* (London: SCM Press, 1961), p. 113.

[11] Jacques Ellul, *Prayer and Modern Man* (New York: Seabury, 1970), p.174.

[12] The fullest account of this is his *To Will and To Do: An Ethical Research for Christians* (Philadelphia: Pilgrim Press, 1969) where (p.108), Ellul asserts, "Every honest reflection must absolutely begin by acknowledging that…there cannot be a Christian ethic". I have discussed this point more fully in my *Living the Word, Resisting the World* (Carlisle: Paternoster Press, 2002), pp. 108-112.

[13] John Howard Yoder, *Nevertheless* (Pennsylvania: Herald Press, 1992), p. 177. n16.

[14] Ronald Ray, *A Critical Examination of Jacques Ellul's Christian Ethic* (unpublished Ph.D., University of St. Andrews, 1973), p. 196, n3.

[15] "acceptable, non condemnable" *(Contre les violents),* p. 170.

[16] "La violence est *toujours* condamnable" (*Les combats de la liberte* (Geneva : Labor et Fides, 1984), p. 166 (italics orignal).

[17] *Jacques Ellul on Religion, Technology and Politics : Conversations with Patrick Troude-Chastenet* (Atlanta : Scholars Press, 1998), p. 39.

[18] Oliver O'Donovan, "War and Peace" in McGrath, Alister (ed), *The Blackwell Encylopedia of Modern Christian Thought* (Oxford, Blackwell, 1993), pp. 655-6.

[19] *The Ethics of Freedom* (London: Mowbrays, 1976), p. 406.

[20] "The distinction between a moral and a non-moral evil can be rendered in terms of what is evil *as action* and what is evil *as suffering.* Not every action that involves the suffering of evil is an evil action. The non-pacifist tradition has represented the justified belligerent as suffering the evil of necessity, but not as doing evil" (O'Donovan, *op. cit.*,p. 655).

[21] I have explored some of these issues a little further in the booklet *When Is War Justified?* (Cambridge: Grove Books, 2003), available from www.grovebooks.co.uk

Beyond Cyberterrorism: Cybersecurity in Everyday Life

by Dal Yong Jin

Dal Yong Jin (daljin@uiuc.edu) has degrees from Yonsei University (B.A. in Public Administration, and M.A. in Public Policy) and the University of Texas-Austin (M.P.A.). He is a Ph.D. candidate in Communications at the University of Illinois-Urbana.

Introduction

The attacks of September 11, 2001 against the United States reflect a growing use of the Internet as a digital and physical against terrorism. Since September 11 many computer and security experts have looked at the issue of cyberterrorism in a new light. Governments throughout the world have come to understand that terrorists and cyber criminals, such as crackers—reckless computer geeks aiming to crack codes, or bring havoc to computer traffic—are using today's information infrastructure to bring havoc to computer traffic and threaten safety. The number, cost, and sophistication of these attacks are rising at alarming rates, with aggregate annual damage worldwide now measured in billions of dollars. The September 11 attacks have awakened the world to consider the real possibility of cyberterrorism.

There are several reasons why the Sept. 11 attacks point to cyberterrorism. One is Osama bin Laden's networks and his use of the Internet to organize the attacks. He used laptops with satellite uplinks and heavily encrypted messages to liaison across national borders with his global underground network even before 2001. The other is the possibility of using steganography, a means by which one can hide messages in digital photographs or in music files but leave no outward trace that the files were altered. Osama bin Laden reportedly used steganography to conceal his messages for the September 11 attacks ("Veiled Messages," 2001).

Moreover, concerns heightened that future cyber and physical attacks—not just for human targets, but for the telecommunication infrastructure as well—might be combined. Many New York citizens indeed could not use telecommunication and online systems for hours after the terrorist attacks due not only to overload but also destruction of the telecommunication infrastructure—including that in the World Trade Center. At that time, the United States narrowly avoided a complete shutdown of its critical financial transaction system—the nation's mechanism for electronically transferring funds (Scott, 2002).

Such threats existed before the Sept. 11 attacks around the world, but the possibility of a significant attack, specifically, a combined cyber and physical assault, is being taken much more seriously since those events (Thibodeau, 2001).

The growing threat of terrorism, which has become one of the most significant global issues in recent years, raises the specter of increased security risks for information managers—ranging from the nuisance of Web site defacements to the possibility that systems could be targeted in conjunction with a physical attack to maximize disruptions. Computer and security experts fear that cyberspace could be terrorist's next target because they saw a clear warning in the terrorists' reliance on, and expertise in, information technology. It had become clear that the computer communication infrastructure, on which wealth, information, and power in our world depend, is highly vulnerable to intrusion, interference, and disruption. Naturally, cybersecurity measures have come to the attention of governments as the most significant method to protect society from cyberterrorism.

This paper studies the development of the concept of cyberterrorism in cyberspace. In particular, it examines cultural aspects of cyberterrorism to ascertain its characteristics. This paper discusses the specific question of the relationship between cyberspace and cyberterrorism, as well as several cultural aspects, such as the relationship between humans and technology, and privacy. Then this paper addresses the significance of cybersecurity for protecting our society from cyberterrorism. Finally, it analyzes the importance of cybersurveillance and discusses the function of encryption as a valuable cybersecurity tool in everyday life in a digital society.

Cyberterrorism in Cyberspace

In the wake of the September11 attacks, many scholars, computer experts, and government officials around the world quickly jumped to conclusions that a new breed of terrorism is on the rise and that society must defend itself with all possible means. They understand that cyberattacks are sufficiently destructive to generate fear comparable to that of physical terrorism. Attacks that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or major economic losses are examples.

Before developing the concept of cyberterrorism, however, it is necessary to explain the concept of terrorism. Computer experts and government officials borrowed the definition of terrorism to explain cyberterrorism, though no one definition of terrorism has gained universal acceptance. Brian Jenkins (1996), a former advisor to the National Commission on Terrorism, described terrorism as the calculated use of violence such as fear, intimidation or coercion, or the threat of such violence to attain goals that are political, religious, or ideological in nature. The U.S. Department of State (1996) defined terrorism as premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents. Meanwhile, Noam Chomsky used the term terrorism as the use of coercive means aimed at civilian populations in an effort to achieve political, religious, or other aims. He explains the World Trade Center bombing as an example of this kind of particularly horrifying terrorist crime (Barsamian, 2001, p.19).

Many security experts borrowed these different definitions to explain cyberterrorism; however they cannot agree on one single definition on cyberterrorism because terrorism in cyberspace is difficult to define. Among these, Barry Collin (1996), a senior research fellow at the Institute for Security and Intelligence in California, defined cyberterrorism as the convergence of cybernetics and terrorism. The United States Federal Bureau of Investigation defines it as any politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents. Possible cyberterrorism targets, therefore, include the banking industry, military installations, power plants, air traffic control centers, and water systems (Cyberterrorism, 2001). Hence, cyberterrorism is sometimes referred to as electronic terrorism, netwar or information war. Cyberterrorism represents a new stage in that it occurs in and with cyberspace, and means an attack on the information structure and function. Examples of cyberterrorist activity include use of information technology to organize and carry out attacks, support group activities and perception-management campaigns. Depending on their impact, attacks against critical infrastructures such as electric power or emergency services could be acts of cyberterrorism. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not be (Denning, 2002). In other words, the potential impact of cyberterrorism on private corporations and government agencies goes well beyond the traditional civil and criminal definitions of damage.

The damage from cyberterrorism has not been viewed only in physical terms. In this regard, computer and security experts assess the probability of various types of cyberattacks, which will occur in the near future:

- Very likely: Electronic warfare is the threat feared most. It could come in the form of denial-of-service attacks, in which crackers overwhelm and disable Web sites with junk data. Other electronic attacks include computer worms and viruses—malicious computer programs that spread via the Internet and erase computer data or clog Internet traffic ("Experts fear," 2001). Online harassment such as harassing email, unsolicited pornographic pictures, and online stalking is also included.
- Likely: State-sponsored computer warfare is aimed at mainly the U.S. although it targets other countries. More than 30 countries have developed asymmetrical warfare strategies targeting vulnerabilities in U.S. computer systems. Because of U.S. military superiority, the countries see electronic warfare as their best tool to puncture U.S. defenses.
- Unlikely: The cutting of hundreds of fiber-optic cables—which carry Internet traffic between major hubs—knocks out portions of the Internet. Such an operation would require intimate knowledge of where key data hubs are, which only a handful of Internet firms know. It also would require a Herculean effort: most fiber cables are underwater or buried underground, so they are not easy to attack.
- Very unlikely: The bombing of Internet facilities, such as major data hubs, cripples the Internet. However, it is nearly impossible because the Internet resembles a cobweb of geographically dispersed facilities. For instance, in the United States, there are major routing hubs in Silicon Valley, Washington, Chicago, and Dallas ("Experts fear," 2001). Likewise, Ericsson world network is centered in Sweden, the Nokia world network is centered in Finland, and the NEC world network is centered in Japan.

As can be seen in this dichotomy, computer and security experts do not take seriously the connection between computer and physical attacks, i.e., attacks on human beings. Terrorists could coordinate a cyber attack with other forms of attacks against physical infrastructure, such as those on September 11. For computer and security experts, however, the main defense against cyberterrorism is to protect the information infrastructure. Cyberterrorism could be understood as a means to attack computer systems and infrastructure rather than to attack people.

Cultural Aspects of Cyberterrorism

It is generally recognized that technological decisions are made first, and then reflect on them ethically after they are developed. Throughout the history of technological innovations its main architects have often denied their moral responsibility. In this frame of mind their solutions do not require any ethical reflection. In fact, many users of technology argue that technology is essentially amoral and an entity apart from values. They point out that, if people use technology for destruction or pollution, as in the case of nuclear weapons and chemical pollution, it should not be blamed on technology, but on its misuse by politicians, the military, big business and others.

However, the historical emergence of a technological culture has made the issue of moral responsibility for technological development increasingly urgent because technology inevitably brings significant risks, as well as great benefits. Computer and cyberspace, in which cyberterrorism occurs, also brings about risks because they were not created by sheer act of will. Computers and the Internet indeed draw attention to the commercial, political, and military interests from the beginning. Therefore, it is indispensable to seriously consider the human and social aspects of cyberterrorism in cyberspace. As Jacques Ellul (1964) emphasized, one should be looking at technology in its sociological aspect because technology is not an isolated fact in society but is related to every factor in the life of modern man. With Ellul, Clifford Christians (1989, pp. 124-125) points out, "technology is the distinct cultural activity in which human beings form and transform natural reality for practical ends with the aid of tools and procedures." He argues that cultures are humankind's distinctive and immediate environment built from the material order by men and women's creative effort.

In this light, cyberterrorism could be understood based upon the relationship between man and technology. It requires understanding the relationship between communications and control together because cyberterrorism affects the relationship between communication technology and the humans who handle it. As Norbert Wiener argued (1957, p.16), society can only be understood through a study of the messages and the communication facilities which belong to it; and that in the future development of these messages and communication facilities, messages between humans and machines, between machines and humans, and between machine and machine, are destined to play an ever-increasing part. Indeed, communication and control belong to the essence of a person's inner life, even as they belong to our social life.

Regarding the relationship between people and technology, cyberterrorism occurs when humans use potentially harmful aspects of the technology. Cyberterrorism occurs because some consider cyberspace as a zone of unlimited freedom, a reference grid for free experimentation, an atmosphere in which there is no barrier (Robins and Webster, 1999, p.91). For instance, crackers try—without permission—to enter computer systems by breaking through security measures. Breaking into a computer system with criminal intentions is illegal and a case for criminal prosecution.

Meanwhile, cyberspace is a geographically unlimited, non-physical domain, in which—independent of time, distance and location—transactions take place between people, between computers, and between people and computers. Unlike physical attacks, cyberattacks are carried out from the comfort of their home and can occur in more than one place at a time through cyberspace. Cyberspace enables terrorist organizations to plan attacks more easily on multiple targets and spread their own organizations over a larger geographic area. It is not closed, but open—where we live everyday. To cyberterrorists, distance is meaningless. The Internet provides them with the ability to be halfway around the world instantly, in many places at once, and have an army of compromised machines to do their bidding (Robinson, 2001, pp.17-20).

In fact, one characteristic of cyberspace is the impossibility of pointing to the precise place and time where an activity occurs or information traffic happens to be. As Lefebvre observes, space and time are intertwined in nature and in society, and space organizes time in a network society (Lefebvre & Nicholson, 1991). This is possible because cyberspace plays a fundamental role in altering the nature of information's production, distribution, and consumption by allowing radically greater amounts and speeds of information flow (Jordan, 1999, p.117). Since more and more objects are provided via digital facilities, they acquire forms of intelligence, can communicate with each other, and thus create a permanent virtual space in which time and space lose their absolute significance. The spaces of the physical and the virtual world are closely interconnected.

Naturally, the threat of cyberterrorism, which has these cultural forms mentioned above, has increased with the development of computers, the Internet, and broadband because Internet communication allows terrorists to be decentralized, and thus harder to identify and observe their attacks. By the end of 2001, there were 455 million computers around the world. Internet users have also increased 17.5-fold between 1994 and 2002, from 38 million in 1994 to 665 million in 2002 (Computer Industry Almanac Inc, 2002). In the U.S. alone, almost 160 million United States households and businesses used the Internet for communication and commerce in 2002. With the rapid growth of computing and online systems, almost $2.2 trillion in goods and services were sold via the Internet in 2001. That is expected to grow to $12.2 trillion in 2006 (UN Conference on Trade and Development, 2002). Furthermore, every day, 1.4 billion emails were sent in 2001(Swartz, 2001).

Under these circumstances, the number of cyberattacks rose to almost 35,000 during the first three quarters of 2001 alone, from 21,756 in 2000, and 2,134 in 1997, respectively. Among these, the Love Bug virus hit over 55 million computers and crippled email systems around the world in May 2000. Approximately four percent of the total computers that received the virus required human intervention to reconfigure them or in some way repair them, which resulted in $10 billion in economic damage. The Code Red worm also infected about a million servers in July and August in 2001 and caused $2.6 billion in damages (Denning, 2002). Cyberattacks caused $12 billion in damage and economic losses in 2001 alone (Squitieri, 2002).

The number and damage of cyberattacks worldwide is growing with the development of broadband (high speed Internet services) in recent years. Broadband users are seen as being more vulnerable to attacks because their computers are always connected to the Internet. In particular, several East Asian countries, which are showing rapid growth of broadband, produce the most cyberattacks of any country apart from the U.S. Asian and Pacific Rim countries indeed produced 91 percent of all attacks during the fourth quarter of 2001. Among these, computer-related crime in Korea, which boasts 10 million broadband users, soared. Computer-related crimes in Korea zoomed 13.6 times higher to 33,289 cases in 2001 from 2,444 a year earlier (National Policy Agency, 2002).

The next generation of terrorists will grow up in a digital world, with ever more powerful and easy-to-use cracking tools at their disposal. They may see greater potential for cyberterrorism than do the terrorists of today, and their level of knowledge and skill relating to cracking will be greater. Cyberterrorism could also become more attractive as the real and virtual worlds become more closely coupled with automobiles, appliances, and other devices attached to the Internet. Unless these systems are carefully secured, conducting an operation that physically harms someone may be as easy as penetrating a Web site is today. In other words, societies that apply many digital systems are extremely vulnerable to cyberterrorism. With relatively simple tools the key functions of such societies can be disrupted. Therefore, cybersecurity is the essential topic in current debates on new forms of war on terrorism because the relationship between men and technology must be secure.

Cybersecurity in Everyday Life

Security risks in digital systems can be caused by totally unpredictable factors, such as earthquakes, floods, fires, and lightning as well as cyberterrorism. Security can also be threatened by electromagnetic signals that suddenly open or close electronic gates and doors or set electronic toys in motion (Hamelink, 2000, p.116). However, the government and business have not paid much attention to security until recent years. In the business sector, corporations have spent billions of dollars for electronic security in recent years, however, companies spent, on average, only about $250 for security measures out of every $1 million they spent on information technology in 2001 (Lemke, 2002, p.31). At the government level, the situation was not far different. For instance, the United States government spent $938 million in 2000 to protect federal computer systems.

Increased security concerns in the wake of the September11 attacks have stimulated spending for cybersecurity. The U.S. government sought about $4.5 billion in its 2003 budget request, which accounts for 8 percent of its information technology budget (Berkowitz & Hahn, 2003). Despite tight information technology spending budgets, the worldwide security software market was also projected to be at $4.3 billion in 2002, an 18 percent increases over revenue of $3.6 billion in 2001, according to Dataquest Inc. (2002). Meanwhile, the U.S. government created the Department of Homeland Security for protecting the country from both physical terrorism and cyberterrorism in November 2002. The department would have about 170,000 employees and $37 billion budget. In addition, the U.S. and U.K. homeland security teams are to hold joint exercises as part of efforts to prevent simultaneous cyber terror attacks on the two countries beginning in April 2003.

Alarmed by the September11 attacks, government and security experts are clamoring for the world to craft better cyberdefenses. They want tougher laws against crackers, more resources, and closer cooperation among agencies to thwart attacks. As noted, they worry that the threat of cyberattacks will grow seriously as business and government use the Internet more. They point out that society needs cybersecurity tools and control strategies for society’s security. In fact, cybersecurity issues are so much an intrinsic part of everyday life today because most of our social encounters and almost all our economic transactions are subject to electronic recording, checking, and authorization. For instance, we unblinkingly produce passports for scanners to read at airports, feed plastic cards with personal identifiers into street bank machines, fill out warranty forms when we buy appliances, key confidential data into online transactions, or use bar-coded keys to enter offices and laboratories. However, the growth of electronic commerce and electronic recording has brought about several negative effects for society, such as property damage, and business disruption through online fraud. As Robins and Webster addressed (1999, p.122) information is thought to be the key to a new phase of economic growth, but it also causes severe damage for today’s information society.

As for computerized surveillance and security issues, one of the most important is encryption. Encryption is the art of scrambling messages to a predefined code or key and thus ensuring only those who know the key can read the message. Encryption technology empowers users to protect their digital property from unauthorized use because only the intended recipient—the key holder—can access the information. In particular, the public key approach is the most powerful method of authentication. Two sets of keys are used. In the public key system, one key is publicly revealed and the other is known only to the user. The keys are linked in such a manner that information encrypted by the public key can only be deciphered by the corresponding private key. Specifically, the public key (the product) is used to encrypt a message. A message encrypted with the public key cannot be decrypted with the same key; only the corresponding private key may decrypt it.

In conventional correspondence two devices are employed to ensure security and authentication. For privacy purposes, it is customary to place a letter within an envelope. But we want the intended recipient to know that we sent the letter, not some impostor. When we sign a letter, that signature serves to confirm our identity. This is exactly what occurs in public key encryption. By applying the recipient's public key to the message, we are assured that only recipients read it.

As the significance of the Internet increases, encryption policy becomes more critical in transferring and protecting information. Under an open and non-secure Internet system, the issue of encryption places emphasis on security, authenticity, identification, and validation in information exchange. For instance, as an effort to prevent unauthorized access or modification and to secure Internet commerce, the U.S. government indicates that a secure Global Information Infrastructure (GII) should incorporate the following aspects:

- Secure and reliable telecommunications networks.
- Effective means for protecting the information systems attached to those networks.
- Effective means for authenticating and ensuring confidentiality of electronic information to protect data from unauthorized use.
- Well-trained GII users who understand how to protect their systems and data (U.S. Government, 2000).

In order to ascertain the characteristics and merits of cybersurveillance, it is worth comparing cybersurveillance with electronics-based surveillance technology, such as Closed-Circuit TV (CCTV) technology. Electronic-based surveillance technologies are recognized as the primary surveillance technologies today. They are very useful tools in prohibiting some teenagers from entering shopping malls for shoplifting or displacing them from certain city streets. The recent growth in the use of the open-street CCTV system has been accompanied by a proliferation in the use of visual surveillance in a wide range of different institutional settings, including hospitals, schools, high rise housing blocks, and the workplace (McCahill, 1998, p.44). It is useful because cameras in public places may deter criminals. However, CCTV surveillance is not useful in cyberspace because it is not a cybersurveillance tool that functions in cyberspace.

CCTV also raises concern about privacy. While CCTV is a useful tool for protecting shoplifting in department stores, it also keeps watch over every guest without their permission. While some government agencies and businessmen believe surveillance is more important than privacy in order to protect physical property and even life, privacy is actually part of the problem (Lyon, 2001, p.66). Hence, in many countries electronic surveillance is mushrooming; however, the sanctity of privacy has also been eroded by the increasing intrusion of surveillance technology. Although safety and security are important, privacy should not be sacrificed for society's safety.

In addition, electronic surveillance is not adequate to protect global data and money flows. As seen thus far, protecting global data and money flow in a digital society should be one of the main functions of surveillance and cybersecurity. As global flow of technology, information, people, images and symbols rise in volume, surveillance should be employed to track and monitor these movements. More delicate and effective surveillance tools, such as high level encryption technology, become essential for protecting our lives and our property.

Unlike CCTV, encryption tools reduce threats to an invasion of privacy while protecting global data and money flows. Considering personal privacy, encryption applies to medical records, personal credit ratings, and spending histories. The problems of failing security need urgent solutions, in particular, for the success of digital trading. The combination of security, privacy, and authentication should make electronic commerce, whether conducted on private networks, the Internet or even in person, the preferred medium for financial transactions of all sorts. The widespread use of encryption is necessary for safe financial transactions online (Jordan, 1999). More importantly, strong encryption hinders cyberterror because terrorists cannot interpret the message easily. Although some terrorists have some decoding skills, it is not easy for them to overcome the encoding skills of security experts. One of the most obvious signs of surveillance is the overhead "electronic eye" of the closed-circuit television camera, and encryption is one of the most effective "cyber eyes" of cyberspace. With these forces behind it, strong encryption might be thought of as an essential element of cyberspace.

Conclusion

Cyberterrorism is becoming a common phenomenon. The next terrorist attack may be not physical in nature but could come through cyberspace to disrupt the communication infrastructure. Cyberattacks on the military, economic and telecommunications infrastructure around the world can be launched from anywhere in the world, and they can be used to transport the problems of a distant conflict directly to America's heartland, as well as other countries. However, it is true that the impact of this risk to the physical health of humankind is still minimal, at present, although the current state of cyberspace is such that information is seriously at risk. Computers do not currently control sufficient physical processes, without human intervention, to pose a significant risk of terrorism in the classic sense. Therefore, a proactive approach to protecting the information infrastructure is indispensable for preventing its becoming more seriously vulnerable.

Computer-based security technology, in particular high-level encryption, is strongly needed for securing today's society from terrorist attacks. Encryption is essential to protect the telecommunication infrastructure. This has obvious advantages for users' privacy, and it deters the members of criminal organizations accessing secret communication. Surveillance and security are not simply coercive and controlling. They are often a matter of influence and persuasion. We are all involved in our own surveillance as we leave the tracks and traces that are sensed and surveyed by different surveillance agencies. Encryption is a non-coercive security and surveillance technique in cyberspace.

In conclusion, cyberterror and cybersecurity have become part of our everyday lives. Everyday life has been conducted more and more in cyberspace in modern times, and this has strong implications for surveillance. On a daily basis, life in cyberspace entails surveillance in constantly increasing contexts.

References

Barsamian, D. (2001). "The United States is a Leading Terrorist State: An Interview with Noam Chomsky by David Barsamian." *Monthly Review*, 53 (6), 10-19.

Berkowitz, B., & Hahn, R. (2003). "Cybersecurity: Who's watching the Store?" *Issues: In Science and Technology (Spring 2003)*, 1-12.

Christians, C. (1989). "A Theory of Normative Technology." In Byrne, E., & Dordrecht, J. Pit. (Eds.). *Technological Transformation: Contextual and Conceptual Implications*. Netherlands: Kluwer Academic Publishers.

Collin, B. (1996). The Future of Cyber-Terrorism. Proceedings of 11th Annual International Symposium on Criminal Justice Issues. Chicago: The University of Illinois at Chicago.

Computer Industry Almanac Inc., (2002, December 16). USA tops 160M Internet Users (press release).

Cyberterrorism (2001). Retrieved from: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci771061,00.html

Dataquest Inc. (2002). Security Software Market will Grow 18 percent in 2002 (press release).

Denning, D. (2002). *Is Cyber Terror Next*? Retrieved from: http://www.ssrc.org/sept11/essays/denning.htm

Ellul, J. (1964). *The Technological Society*. New York: Vintage.

"Experts Fear Cyberspace Could Be Terrorist's Next Target." (2001, October 9).*USA Today*, B1.

Jenkins, B. (1996). *The Future Coverage of International Terrorism*. Retrieved from: http://www.wfs.org/jenkins.htm

Jordan, T. (1999). *Cyberpower: The Culture and Politics of Cyberspace and the Internet.* New York: Routledge.

Hamelink, C. (2000). *The Ethics of Cyberspace*. London: Sage.

Lefebvre, H., & Nicholson, D. (1991). *The Production of Space*. New York: New York University Press.

Lemke, T. (2002). "Cyber-terror a certainty, and government is most Vulnerable." *Insight on the News*, 31 (1).

Lyon, D. (2001). *Surveillance Society: Monitory Everyday Life*. Philadelphia: Open University Press.

McCahill, M. (1998). "Beyond Foucault: Towards a Contemporary Theory of Surveillance." In Norris, C., Moran, J., & Armstrong, G. (Eds.). *Surveillance,Closed Circuit Television and Social Control* (pp.41-65).

National Police Agency. (2002). *2002 Policy White Paper.* Seoul: National PolicyAgency.

Robins, K., & Webster, F. (1999). *Times of the Technoculture: From the Information Society to the Virtual Life.* London: Routledge.

Robinson, C. (2001). "Physical Disaster Propels Cybersecurity Initiatives." *Signal*, 56 (3).

Scott, W. (2002). "Nation's Inforsec Gaps Given New Scrutiny Post-Set.11." *Aviation Week & Space*, 59-61.

Squitieri, T. (2002, May 6). "Cyberspace full of terror targets." *USA Today.*

Thibodeau, P. (2001, September 24). "War against Terrorism raises IT Security Stakes." *Computer world*, 39.

United Nations Conference on Trade and Development. (2002). E-Commerce and Development Report. (New York: UNCTAD).

U.S. Department of State. (1996). *Patterns of Global Terrorism Report*. Retrieved from http://www.state.gov/www/global/terrorism/1996Report/1996index.html.

U.S. Government.(2000). *Whitehouse, A Framework for Global Electronic Commerce*. Retrieved from: http://www.whitehouse.gov/WH/New/Commerce/about.html.

"Veiled Message of Terror may Luck in Cyberspace." (2001, October 30). *New York Times*, F1.

Surveillance After September 11: Ellul and Electronic Profiling

by David Lyon

David Lyon (lyond@post.queensu.ca) is Professor of Sociology and Coordinator of Graduate Studies at Queen's University (Canada). He is also the research director of the international Surveillance Project based at Queen's, investigating surveillance, risk management, and social ordering in global information societies (*http://qsilver.queensu.ca/sociology/Surveillance/intro.htm).*

In a classic one-liner, Jacques Ellul once suggested that "To be sure of apprehending criminals, it is necessary that *everyone* be supervised."[1] Substitute the word "terrorists" for "criminals" and we have an uncannily accurate description of the world since 9/11. Anti-"terrorist" measures, from securing airports to intercepting emails, are everywhere. The dramatic events of 2001 served to accelerate processes of general "supervision" that had been underway since Ellul's prophetic words were written, in the early 1960s. Especially in the USA, but also in countries around the world, we are creating sophisticated surveillance societies in which everyone is supervised, or watched over.

Let me clarify two things right away. One, in this world that we help to make, what I'm calling surveillance is partly a by-product of modern bureaucratic efficiency. More mobility means that many things are done at a distance. So some ways are needed of keeping track of transactions or keeping tabs on populations. Surveillance fills that gap – PINs, barcodes, video images, and scans are tokens of trust that compensate for the fact that in a global village we can't all know everyone else. So surveillance is not just sinister; but neither is it simply benign. It's deeply ambiguous, and increasingly influential. In this piece, however, I focus on the risks.

Two, what follows is not just a paranoid whine about intensified intrusions, still less a plea for more privacy. In the context of today's rampant individualism, the antidote to more surveillance is quickly seen in terms of personal space and personal solutions. Of course, some government departments or corporations have no business prying into our personal affairs, and even traffic light cameras can pick up passenger images that should never be recognizable. But while some aspects of privacy may be important – human dignity based on the imago dei would make self-communication a voluntary, limited activity within relations of trust – the language of privacy fails to touch many crucial issues. As well, privacy is also ambiguous.

Or should domestic violence in a "private" space be exempt from public scrutiny?

9/11 produced a rapid augmenting of existing surveillance trends. Many companies, government departments and organizations (such as the American military) saw 9/11 as an opportunity to put in place measures previously proscribed because of privacy or civil liberties scruples. Multiple use smart cards, for example, have been around for over a decade, but few large scale uses have been found for them. No wonder Larry Ellison, of Oracle Corporation, quickly offered free software to the US government to create a national ID. Mercifully, despite the emotionalism and panic, he was turned down.

This reflects one major trend in surveillance, to automate and integrate systems of processing personal data. What was once done using ranks of filing cabinets and index cards in large offices could be done much more easily with computers. Add telecommunications, so they could network, and software for searching databases, and the stage was set for surveillance in its dominant twenty-first century forms. This isn't the top-down nightmare of eerie telescreens featuring *Nineteen-Eighty-Four*'s Big Brother, but the Google model of homing on hits using keywords. It's algorithmic surveillance, that sorts for suspects.

But not only for suspects. The categories cover all kinds of persons, lifestyles, occupations, interests, positions and preferences. Just as the firm might fire you for failing to meet your performance requirements, the bank may well do the same if your business is worth less to it than your neighbour's. The Royal Bank of Canada does it by sending letters that explain their new financial features, which reveal that not all customers will qualify.

Still, if we're thinking about 9/11, suspects are exactly what surveillance seeks. Indeed, hasty legislation (in the USA and elsewhere) and new surveillance technologies combine to create an expanded version of what Onora O'Neill calls a "culture of suspicion."[2] Vague and prejudicial definitions of "terrorist" help to widen the net, while dubious surveillance softwares serve to tighten the mesh. But those are only the first steps. The culture of suspicion spreads as trust is eroded at every level. New York Muslims called "Mohammed" are finding their American Express cards withdrawn; companies are hiring consultants to do "security" checks on people who apply for jobs; and hotlines proliferate for letting ordinary people be the "eyes and ears" of law enforcement.

Unfortunately for those spending millions on high-tech security devices, the systems aren't really up to snuff. The brand new facial recognition cameras at Logan Airport in Boston, from which two planes containing global guerillas took off on 9/11, have been criticized by an independent security contractor for having blurred shots and excessive false positives.[3] In short, they won't work for the purposes stated. And this is also true of several other surveillance schemes for identifying, locating, and capturing "terrorists."[4]

But while the new surveillance is unlikely to prevent terrorism, this does not mean it is ineffective. Those drawn into the net include a vast range of persons – all of us, one way and another – whose personal data are extracted from us as transaction records (such as phone, credit cards), behaviours (what cameras and scanners see in car parks or airports), body indicators (iris scans or fingerprints), and other traces are transmitted to databases. True, we may falsify records on the internet, or evade the street camera, but most of us comply, cheerfully or otherwise, most days.

Notice what goes into the system. Just bits of data, fragments of information. They may be built into a larger profile but even that will scarcely be recognized as a reliable image by the person concerned. No matter, it's the fragments that count. The system isn't interested in "who" you really are. All it can do is create situational controls, momentary management opportunities. These surveillance devices are meant to channel flows, to inhibit some activities, to promote others. "Entry denied," flashes the sign; "Do you wish to redeem your points?" asks the cashier; "You have been selected…" says the SPAM. Morality does not really feature, here. Mere management has taken over.

This means that we are all targets, and that justice reduces to the actuarial. The smug response that those who have nothing to hide have nothing to fear is pernicious nonsense. The fact of being placed in a category of suspicion, or even in a marketer's niche, means that our life-chances and our choices are already affected. Systems designed to sort are there to classify our lifestyles and our proclivities, discriminating between one and another. Different insurance rates, promotional offers, treatment by police, and speed of passage – such as through airport check-in – are the result. That your neighbourhood becomes high-risk may not be your doing, and that you're a single mother on welfare not your fault. The automated label sticks, until you can find some way of removing it. So much for presumptions of innocence!

But let's go back to those global guerilla fighters. No one wants to see them succeed, and every right thinking person believes, correctly, that terrorism is a curse to be opposed. If reports of capture, whether in Pakistan, Germany, Indonesia or Canada are correct, then one checks in vain for reports of high tech devices being crucial. In fact, where terrorist cells have been busted, or dangerous individuals apprehended, it seems that old-fashioned intelligence-gathering, under-cover work, and informers are responsible.

So why all the hype about technology? Well, this is where Ellul becomes relevant once more. He maintained that in the modern era an obsessive search for the one right way of doing things – the correct "technique" – was fast becoming dominant. Hence his critique of "technological society." Appropriate goals were being obscured as the myopic quest for the best means filled the cultural horizon. The idol would bind its adherents to a single program, and blind them to its consequences and alternatives. "In displacing spirituality," summarises Karim Karim, "technique itself becomes an object of faith."[5]

Of course, Max Weber had made similar observations, much earlier in the twentieth century, but he seemed to despair of ever finding away out of this "iron cage." His insights are indispensable, but incomplete. On the other hand, despite his apparent view that technology is an unstoppable juggernaut, Ellul actually insisted that choices could still be made. Having been a member of the French World War Two resistance movement against the apparently invincible German occupation, his position had some credibility. Ellul parted company with Weber at the crossroads of the spiritual. The latter confessed to being "religiously tone-deaf" while the former pursued parallel paths of sociological and theological analysis.

So what directions are suggested by this line of thinking? The first is a general point about the priority of "technique." From the Renaissance, the idea took root that peace and prosperity could be engineered, and the Enlightenment took this notion further. Technology was among the tools for manufacturing desirable social conditions. But this is an inversion of priorities. Loving one's neighbour and seeking social justice are stressed by the Hebrew scriptures as prior conditions for peace and prosperity. Doing technology falls under the same rubric. It is subject to norms, to morality and to ethics. You can't engineer security or safety, although technology may play an appropriate role in achieving such goals.

Moving closer to the aftermath of 9/11, what might a socio-theological approach have to offer? Assuming there is some merit in the above argument, key issues concern what we might call "embodiment" and "embrace." Why these?

First, the garnering of personal data fragments makes it possible to assemble profiles that proxy for persons. I may not recognize my data-image but it's the data-image that plays a key role in my life-chances. The abstract data-image is not the embodied person, even though it seems to have taken over the task of defining me. In the twenty-first century, electronic proxies are likely to proliferate. Modern(ist) notions of the independent individual are already imperiled by such developments. But at the core of Christian commitment is the notion that persons are relational and embodied. Those relationships, echoing the sociality of God, are central. And our being "enfleshed," which was affirmed by the "enfleshment" (incarnation) of Jesus, is equally so. So whenever a data-image is privileged over the person, damage is done.

Second, the use of searchable databases for surveillance means they act as a form of triage, screening behaviours and activities in order to assign different treatments. It's an exclusionary process that cuts out or creams off without recourse to ethics. Loving one's neighbour flies in the face of this, demanding instead inclusion and embrace. As Miroslav Volf poignantly notes, exclusion may be overt, flowing from domination, or it may be occluded, subtly producing abandonment. [6]In the twenty-first century, we have found ways of automating the practice of "passing by on the other side." As soon as "Arab-Muslim" or "not credit-worthy" features in a database, mental sirens should sound.

None of this is meant to imply that policy makers, politicians, or technologists for that matter, have easy decisions to make. Rather, appropriate priorities should be recovered and highlighted as each issue is confronted. Equally, everyone needs to be informed and involved. In the twenty-first century, the politics of information are shifting to a much more central position than formerly, and democratic citizenship demands that all take an interest in how this plays out. We shall surely get the technologies we deserve if we do not make our voices heard in dissent and re-direction. Already, popular outcry has helped to rein in some of the most egregious aspects of the "Total Terrorist Awareness" and "Computer-Assisted Passenger Pre-Screening" programs in the USA.

Although present surveillance trends were visible well before 9/11, those events have served to accelerate and also to highlight them. Technological decisions are now far too important to be left to politicians and engineers. They affect all of us, and, at a simple level, we can all contribute to shifts in thinking and practice. It behooves those who believe that loving neighbours and seeking justice are key priorities to expose the lie that having "nothing to hide" exempts one from the consequences of today's surveillance. Likewise, the emphasis on justice requires that mere "privacy" solutions be re-thought. Profiling, not prying; sorting not spying; these are the real issues. Whenever someone suggests that "intrusion" is the problem, remember that "exclusion" is at least equally dangerous.

Having begun with some references to Ellul, I'll let him have the last word too. I have no special brief for Ellul; indeed, I am also a critic of some of his ideas. But his insights, developed at the dawn of the computer era, have a compelling resonance with what's happening today. He once commented that in the antique cities of Babylon and Ninevah, peace, prosperity and security were sought through city walls and military machines. But he also reminded readers of another city, where inclusion is the key – the gates are always open – and where the light is always on.[7] Trust, not suspicion, and embrace, not exclusion, are the watchwords. We don't yet see this city. But as another sage once said, it's not too much to hope for.

References

[1] Jacques Ellul, *The Technological Society* (Knopf, 1964), p. 100.

[2] Onora O'Neill , *A Question of Trust* (Cambridge, 2002).

[3] Technology and Liberty Program of the ACLU, Sept. 2, 2003 (www.aclu.org/Privacy/Privacy.cfm)

[4] Details of some such failed schemes are in David Lyon, *Surveillance after September 11* (Polity Press, 2003).

[5] Karim H. Karim, "Cyber-Utopia and the Myth of Paradise: Using Jacques Ellul's work on propaganda to analyse information society rhetoric" *Information, Communication, and Society,* 4:1, 2001, 113-134.

[6] Miroslav Volf, *Exclusion and Embrace* (Abingdon 1996).

[7] Jacques Ellul, *The Meaning of the City* (Eerdmans, 1970).

Make Payments to IJES Electronically?

The IJES office can accept payments only in US dollars because of the huge collection fees otherwise charged by US banks.

A new option in many countries is to go to www.paypal.com and use a credit card to make a payment to "IJES@ellul.org." If you try this option, be sure to note your name, address, and purpose of payment.