

Chapter 22

ICTs and Border Security Policies in the United States and the European Union

Peter Shields

Eastern Washington University, USA

ABSTRACT

ICT-related initiatives have dominated the border security strategies of the United States and the European Union in recent years. One set of surveillance systems fortifies the borderline. Another set is creating new frontiers away from the traditional boundary. The objectives of this chapter are to provide a detailed mapping and critical assessment of this two-pronged approach. With respect to the assessment, two arguments are made. First, there are good reasons to believe the approach is not enabling the authorities to deter identified border threats. Second, the approach is contributing to a border management regime that is having an increasingly divergent impact on the mobility and life chances of different groups and populations. In conclusion, it is suggested the inefficacy of the approach is due to contradictions and blind spots embedded in policy maker's approaches to security issues. Remarks are offered as to why US and EU decision makers emphasize the role of ICTs as they seek to reconstitute their respective borders.

INTRODUCTION

The 9/11 attacks on the World Trade Center and Pentagon and the subsequent terrorist actions in Madrid and London provided the catalyst for a surge of border security initiatives in the United States (US) and the European Union (EU). Deployment of a variety of “state-of-the-art” state-of-the-art information and communication

technologies (ICTs) has been at the heart of this border work. At least two trends characterize this policy preference for increasingly relying on ICT-related border controls. First, myriad surveillance initiatives have been implemented or proposed to fortify or “harden” the various manifestations of the traditional border. For example, the US government's ongoing Secure Border Initiative seeks to build a network of “next generation” detection technologies (e.g., sensors, cameras, radars and unmanned aerial vehicles) along the nation's

DOI: 10.4018/978-1-61520-847-0.ch022

southwestern border to deter or help detain illicit border crossers. In the EU context, the Spanish government's Integrated System of External Surveillance, a maritime border surveillance system that deploys a combination of fixed and mobile detection technologies, also exemplifies this trend.

Second, and more innovatively, a plethora of other surveillance initiatives are involved in the creation of new frontiers away from the traditional boundary. More specifically, these initiatives "push out" from the edges of the territory by deploying anticipatory measures aimed at extensive "pre-inspection" and sorting of individuals, goods and conveyances. In the US context, pre-screening initiatives such as the Secure Electronic Networks for Travelers' Rapid Inspection Program (SENTRI), the Free and Secure Trade Program (FAST) and the US Visitor and Immigrant Status Indicator Technology Program (US-VISIT) illustrate this trend. These programs use a combination of database and biometric technologies to both pre-screen and verify the identity of in-bound travelers. In February 2008, the European Commission called for the deployment of similar pre-screening systems as part of its new Border Package entitled, "Preparing the next steps in border management in the European Union" (Commission of the European Communities, 2008).

Policy makers on both continents have casted this high tech two-pronged approach as fundamental to reconciling the tension between potentially colliding policy imperatives. While the first imperative involves the ramped-up commitment to security and stiffer borders, the second concerns the perceived need to maintain or even increase the velocity of cross-border commerce, with its attendant pressure for more permeable borders. Thus, President Bush justified the two-pronged approach in terms of the need to keep "pace with expanding trade while protecting the United States and its territories from the threats of terrorist attack, illegal immigration, illegal drugs, and other contraband" (Office of the President of the United States, 2003, p. 16). Similarly, Franco Frattini,

EU Commissioner, argued that the approach is necessary "to be one step ahead [of] the increasingly better organized networks of terrorists and criminals who have discovered the lucrative trafficking in human beings, drugs and weapons. Innovative and effective border controls have to strike a difficult balance between ensuring the free movement of a growing number of people across borders and guaranteeing greater security or Europe's citizens" (Frattini, 2008, p. 1).

Focusing on US and EU contexts, this chapter has two objectives. The first goal is to provide a detailed mapping of this two-pronged border security approach. In doing so, the intention is to move beyond two deficiencies in the relevant literature. The first involves a tendency to focus only on one kind of ICT-related security initiative either those that bolster the traditional borderline or those that de-territorialize border controls. The second is the tendency of focusing only on initiatives that have been rolled out on one side of the Atlantic or the other. The first tendency works against producing a comprehensive picture of the role ICTs are playing in US and EU border security policies. The second obscures the fact that US and EU authorities are developing broadly similar ICT-related border security initiatives. This chapter addresses these problems.

The second objective is to critically assess the two-pronged border security approach. The approach assumes information is vital to enhancing security and control. More specifically, the two kinds of ICT-related border security initiatives that constitute the approach assume government actors can progressively annihilate the risk of terrorism and other perceived security problems if they can harness the latest technological developments to gather, process, analyze and share the right bits of information about particular individuals, conveyances and cargo. This perspective equates information with knowledge, the antithesis of uncertainty, a source of transparency and control. This chapter assesses this perspective and the ICT-related border security initiatives it informs.

27 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/icts-border-security-policies-united/45396

Related Content

The Battle Within: An Analysis of Internal Fragmentation in Networked Technologies Based on a Comparison of the DVB-H and T-DMB Mobile Digital Multimedia Broadcasting Standards

Håkon Ursin Steen (2011). *International Journal of IT Standards and Standardization Research* (pp. 50-71).

www.irma-international.org/article/battle-within-analysis-internal-fragmentation/56359

Patents and Standards in the ICT Sector: Are Submarine Patents a Substantive Problem or a Red Herring?

Aura Soininen (2010). *New Applications in IT Standards: Developments and Progress* (pp. 109-146).

www.irma-international.org/chapter/patents-standards-ict-sector/41807

Standardization in Enterprise Inter- and Intraorganizational Integration

K. Kosanke (2005). *International Journal of IT Standards and Standardization Research* (pp. 42-50).

www.irma-international.org/article/standardization-enterprise-inter-intraorganizational-integration/2567

Certified Originality of Digital Contents by the Time Authentication

Masakazu Ohashi and Mayumi Hori (2010). *Information Communication Technology Law, Protection and Access Rights: Global Approaches and Issues* (pp. 67-80).

www.irma-international.org/chapter/certified-originality-digital-contents-time/43488

Consensus Versus Speed

Roy Rada (2000). *Information Technology Standards and Standardization: A Global Perspective* (pp. 19-34).

www.irma-international.org/chapter/consensus-versus-speed/23725