THE RISE OF IWAR: 
IDENTITY, INFORMATION, AND THE INDIVIDUALIZATION 
OF MODERN WARFARE 

Glenn J. Voelz

The attacks of September 11, 2001 (9/11) and 
two extended counterinsurgency campaigns in Iraq 
and Afghanistan presented the United States with 
unconventional adversaries for which it was largely 
unprepared. These opponents did not fight as doctrinal 
formations or within clearly defined operational 
boundaries. Rather, they were organized as loose 
networks, comprised of individuals often indistingui 
shable from surrounding populations. Without 
uniforms and flags, the task of identifying and target 
ing these entities presented an unprecedented opera 
tional challenge for which traditional warfighting ap 
proaches were largely unsuited. In response, the U.S. 
military and the broader national security apparatus 
embarked upon a decade of doctrinal, technical, and 
organizational innovations premised on the idea that 
individual combatants had become a salient national 
security concern and a legitimate object of military 
targeting. Within this new operational paradigm, the 
identification, screening, and targeting of individual 
combatants and their associated networks became the 
central focus for a new mode of state warfare—iWar.

Over the last decade, this approach to warfighting has emphasized the operational tasks of identifying key actors on the battlefield, penetrating their networks, and isolating them from larger populations, and, when necessary, conducting kill/capture operations against high-value insurgent and terrorist targets. This strategy required the adoption of new doctrinal concepts deeply influenced by network analysis theory and the use of identity-base targeting. These methods emphasized analytical approaches based upon the disaggregation of battlefield threats down to the lowest possible component—often the 
individual combatant—and introduced identity as a 
critical signature of military targeting.

Along with new doctrinal concepts, the conflicts of the last decade also generated a range of technology innovations specifically designed for the informational demands of identity-based operations. These included biometrics, expeditionary forensics, and DNA analysis, to name a few. However, the tools and methods of iWar were by no means limited to use on foreign battlefields. On the domestic front, similar technologies have been used to construct an expansive identity-based screening program that has kept borders, transportation networks, and American cities remarkably safe since 9/11. This achievement depended upon the accumulation of a dense informational base layer designed to support identity management, network analysis, and data sharing across the entire U.S. national security apparatus.

The challenges presented by post-9/11 adversaries were also the catalyst for a major bureaucratic transformation that has gradually eroded many of the traditional lines separating military operations, foreign intelligence activities, and domestic security functions. These changes reflect a new strategic calculus that has placed the threat from nonstate actors and individual combatants on equal footing with adversarial states in the crafting of U.S. national security policy and as a driver of military innovation. This monograph examines the course of this doctrinal and technical transformation over the last decade and considers the implications for the future of U.S. national security strategy and military conflict in the age of iWar.
More information about the programs of the Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press may be found on the Institute’s homepage at www.StrategicStudiesInstitute.army.mil.

Organizations interested in reprinting this or other SSI and USAWC Press executive summaries should contact the Editor for Production via email at SSI_Publishing@conus.army.mil. All organizations granted this right must include the following statement: “Reprinted with permission of the Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College.”