

Terrorism Open Source Intelligence Report (TOSIR) No. 416 31 December 2009

Contents

[Article 1](#) **“Understanding History’s Seven Stages of Jihad,”** by Sebastian Gorka, [CTC Sentinel](#) (Combating Terrorism Center at West Point), Vol. 2, No. 10, October 2009. *The post-9/11 debate on the meaning of “jihad” has often floundered at a superficial understanding of the term. However, jihad must be understood to consist of four varieties of human activity agreed upon by Islamic theologians and jurists. Since the days of the Prophet Muhammad one of these, jihad by the sword, has been shaped by seven historically-shaped political conceptualizations of jihad. To properly understand the historic significance of Al-Qaeda, it is relevant to review the contextual evolution of the concept of jihad and the great success Al-Qaeda has had in redefining it for the current conflict.*

[Article 2](#) **“Countering the Counter-Terrorists: Senior Jihadis Offer Advice on Security Techniques,”** by Abdul Hameed Bakier, [Terrorism Monitor](#), Vol. 7, No. 11, 30 April 2009. *In a quest to spread security and military knowledge that is vital for successful Salafi-jihadi terror operations, jihadi Internet forums intermittently release training lessons in all kinds of subjects. This article examines two types of jihadi security training materials. The first training episode, published by Al-Qaeda in the South Arabian Peninsula, tutors jihadis on ways to resist interrogation. The second episode discusses intelligence and security techniques and was prepared by an Ingush jihadi who is an Arab field commander operating in Chechnya. Although more advanced jihadi training materials have been made available on the Internet, the “General Security Advice” prepared by the Ingush jihadi was posted in almost all Salafi-jihadi forums and blogs to depict a united Salafi-jihadi global front.*

[Article 3](#) **“Crime and Terrorism,”** by Colonel Robert B. Killebrew, U.S. Army (Ret.), [Small Wars Journal](#), 2009. *In the eight years since the United States has been at war in Iraq and Afghanistan there have been some profound changes in the structure of global terrorism, particularly with regard to the relationship between terrorist movements and international crime. The indisputable convergence of terrorism and international drug trafficking is playing out before our very eyes in Afghanistan, and in many other places around the globe. The scope of the estimated 1.5 trillion dollars in illicit money being raised around the world, infused into the global monetary stream, and manipulated by criminals threatens to undermine the stability of the international order itself, striking at financial and banking systems and undermining legal and political authority in legitimate states. Against such deterioration, terrorism is only a subset of a larger problem of illegality and aggression against the underpinnings of civil society itself,*

[Article 4](#) **“Securing the Information Highway: How to Enhance the United States’ Electronic Defenses,”** by Wesley K. Clark and Peter L. Levin, [Foreign Affairs](#), November-December 2009. *The cybersecurity threat is real. Adversaries can target networks, application software, operating systems, and even the ubiquitous silicon chips inside computers, which are the bedrock of the United States’ public and private infrastructure. All evidence indicates that the country’s defenses are already being pounded, and the need to extend protection from computer networks and software to computer hardware is urgent. The U.S. government can no longer afford to ignore the threat from computer-savvy rivals or technologically advanced terrorist groups, because the consequences of a major breach would be catastrophic.*

[Top of TOSIR Cover Page](#)

Articles

Article 1 [Return to TOSIR Cover Page](#)

1. **“Understanding History’s Seven Stages of Jihad,”** by Sebastian Gorka, **CTC Sentinel** (Combating Terrorism Center at West Point), Vol. 2, No. 10, October 2009. [KBTZJihad, KBTZDefinitions, KBTZIslam, KBTQStrategy] Dr. Sebastian Gorka teaches irregular warfare and counterterrorism at the College of International Security Affairs of the National Defense University; and is an associate fellow of the Joint Special Operations University. We *quote* from <http://www.ctc.usma.edu/sentinel/CTCSentinel-Vol2Iss10.pdf>:

The post-9/11 debate on the meaning of “jihad” has often floundered at a superficial understanding of the term. Jihad is often simply referred to as either “striving” or “holy war.” Jihad, however, **must be understood to consist of four varieties of human activity** agreed upon by Islamic theologians and jurists. **The first is the jihad of the heart, the so-called “greater jihad” of fighting evil within oneself. The second and third definitions involve the jihads of the mind and tongue,** the condoning of “right” behavior in others and counseling those who have gone astray. **Finally, there is jihad of the sword.** Jihad of the sword is most relevant for the counterterrorism community today because it rests at the foundation of the global jihadist ideology.

[Jihad of the sword contextualized over centuries to fill real, specific, and political needs]

The concept of jihad of the sword has been repeatedly reinterpreted and redefined since the days of the Prophet Muhammad. During this extensive time period, jihad by the sword has been used by protagonists to rally co-religionists in the pursuit of a political objective. **Al-Qaeda and the broader Salafi-jihadi movement have also reinterpreted this concept to justify the direct targeting of civilians in terrorist attacks.**

To properly understand the historic significance of Al-Qaeda, **it is relevant to review the contextual evolution of the concept of jihad** and the great success Al-Qaeda has had in redefining it for the current conflict.

Since the days of the Prophet Muhammad, **jihad by the sword has been shaped by seven historically-shaped political conceptualizations of jihad, occurring in the following order:** [a] **empire building;** [b] **the suppression of apostate subjects;** [c] **the revolution against “false” Muslim leaders;** [d] **the anti-colonial struggle and “purification” of the religion;** [e] **countering Western influence and *jahiliyya*** [*jahiliyya* refers to the age of polytheism and “unbelief” that existed before the Prophet Muhammad]; [f] **guerrilla warfare against secular invaders;** and finally [g] **the direct targeting of civilians in terrorist attacks.** This article will identify each contextual interpretation and the significance of jihad as terrorism.

Each of the contextualizations of jihad of the sword has been dictated by the desire to have jihad fill a real, specific, and political need for Muslims in a given age and facing a specific threat. When the Prophet Muhammad was building a completely new state, he used the concept of jihad to justify the expansion of Islam. **Although the Qur'an does not use the term jihad to refer directly to empire-building in the military sense, sura 25/verse 52 stipulates "obey not the disbelievers, but strive against them with the utmost endeavor."**

[The seventh political definition of jihad is terrorism]

[1] Understood in the context of Muhammad's return [*hijra*] to Mecca from Medina, and the ensuing conflict with the Meccans that is reflected in the latter half of an earlier sura, it is clear that striving is in this instance connected to military combat post-*hijra*, as Muhammad returns to Mecca and enforces his new writ. This constitutes the first offensive use of the concept, referring to the conflict to establish order among the Arab tribes around Mecca, through the use of force if necessary.

[2] When Muhammad's successor, Abu Bakr, faced recalcitrant tribes on the Arabian Peninsula that were threatening the order Muhammad had previously established, the second meaning of jihad was born: *ridda*, or the war against apostasy, against one's own subjects. In the Western world, this would be equivalent to a war against rebels.

[3] The third contextual definition of jihad came centuries later after the eclipse of the Abbasid Caliphate's strength, starting in the second half of the thirteenth century. It is this reworking of the meaning of holy war, most significantly by **Ibn Taymiyya** [Muslim scholar, 1263-1328), that has **the greatest consequence for today's context.** **The motivation for this redefinition was the need to provide Muslims with the right to revolt against their own leaders, specifically the Mongols.** Islam had previously prohibited revolution against Muslim rulers.

Ibn Taymiyya's answer was to remove the prohibition; **he argued that jihad is permissible against one's own leaders if they do not live as true Muslims and if their rule does not conform to the requirements of sharia.** . . . [In] the Middle Ages jihad became legitimate revolution based upon a new mechanism by which the people could denounce their leaders as un-Islamic.

[4] The fourth political reconceptualization of jihad occurred four centuries later, starting in the early 1700s. As the European powers pushed militarily and politically into North Africa, the Middle East, and the Indian subcontinent, the threat to Islamic societies was two-fold. Empires such as the British had to be **physically resisted.** At the same time, **the West's cultural influence** upon the purity of the Islamic faith was growing and had to be countered. During this period, **jihad was defined as anti-colonial resistance.**

This new interpretation of jihad was typified by **the pronouncements of Muhammad ibn Abd al-Wahhab, the founder of Wahhabi Islam.** Its practical and military consequences were amply **demonstrated during the decade-long resistance to the 1830 French invasion of Algeria** led by Abd al-Qadir and **also by the Sudanese resistance to the British** led by the self-proclaimed *mahdi*, Muhammad Ahmad. The

second, non-military element of this redefinition of jihad—what author Noor Mohammad has described as Islam’s internal “housecleaning”—was **represented by Shah Waliullah’s call to spiritual revival and the purification of India’s Muslims under British control.**

[5] This definition of jihad would lead directly to the next interpretation, one that relies heavily on the principles laid down hundreds of years prior by Ibn Taymiyya, including the doctrine of *takfir* (excommunication). **This fifth version of jihad was fathered and later developed by Abu al-A la Mawdudi in India (then later Pakistan) and Sayyid Qutb in Egypt. This time the threat was embodied by the post-World War II Arab leaders of the Middle East and the influence of Western “soft power,”** which together equaled a new *jahiliyya*, or age of polytheism and ignorance. **Apostate leaders were to be resisted once more (and removed if possible), Islam purified and sharia re-imposed.**

[6] **With the invasion of Afghanistan by the Soviet Union in 1979, jihad would no longer be limited to resistance against the cultural and political influence of the secular West or un-Islamic Arab rulers.** Although it is true that within Afghanistan, among the Afghans, the motivation to resist Soviet domination did not have to be couched in terms of theology but simply in terms of survival and sovereignty, **to the Arab mujahideen recruited by the Palestinian Abdullah Azzam, jihad was a crucial concept, a brand Azzam assiduously built in his travels around the world. Most importantly, Azzam built his jihadist brand in a way that negated earlier requirements for holy war to be declared by a legitimate authority, as he redefined military resistance as an individual duty. . . .**

Azzam invoked Ibn Taymiyya by name to justify his version of self-declared jihad and then warned his audiences of the price they would pay if they did not follow the path of military resistance. . . . **By the late-1980s, Azzam’s rebranding of Muslim holy war in a new political and geostrategic context was so successful that even in the West jihad would become synonymous with guerrilla resistance to Communist invasion and dictatorship.**

[7] Only after the eventual defeat of the Soviets, the end of the Cold War, and the outbreak of the first Gulf War would **the seventh and most important redefining of jihad of the sword** be born. **With Azzam’s death in 1989, his organization of Arab guerrillas, the Mujahideen Services Bureau (MAK), was taken over by his deputy Osama bin Laden. Rejected by his own government when he offered to protect Saudi Arabia from Iraq with his Arab fighters,** bin Laden would change the mission and name of his organization. The “godless” Russians had been defeated, the bipolar world order replaced by the hegemony of a victorious United States, a country that had been invited to bring its troops and influence into the Arabian Peninsula to defend Saudi Arabia from Iraq. **Guerrilla warfare within Saudi Arabia against the apostate House of Saud and against U.S. targets was impractical, if not impossible.**

Several influential figures who had followed the teachings of the original Muslim Brotherhood and its leader Hassan al-Banna, including [Al-Qaeda number two] Ayman al-Zawahiri, had, **after the severe crackdown against the Muslim Brotherhood in Egypt, joined the MAK. Bin Laden’s Wahhabi understanding of jihad would be suffused with the ideology of the Egyptian Qutbists. What resulted was Al-Qaeda and a new indirect approach to violent jihad.**

Subsequently, **the meaning of jihad was expanded for a seventh time** since Muhammad built his empire in the seventh century. **The fight would be focused less on irregular warfare in countries where Muslims were suffering and more on the “far enemy,”** which they identified as supporters of tyrannical regimes in the Muslim world. With the East Africa embassy bombings, the USS Cole attack, and then finally the 11 September attacks on New York and Washington, **bin Laden successfully defined jihad as willful targeting of civilians by a non-state actor through unconventional means. The seventh political definition of jihad, therefore, is terrorism.**

[Meaning of violent jihad shaped over centuries to fit needs of those espousing holy war]

It is crucial for analysts and strategic planners to fully understand this mutation and evolution of the concept of jihad over time. It is incorrect to see jihad solely as a religious concept referring to the striving of the individual to be pure, because jihad of the sword is referenced in the *hadith* in multiple instances. **It is clear that the meaning of violent jihad has been shaped during the centuries to fit the needs of those espousing holy war and calling their co-religionists to the battlefield.**

Osama bin Laden’s great historical significance is that he managed to turn jihad from referring to guerrilla resistance against military oppression of the 1980s to mean the killing of mass numbers of civilians on the soil of non-Muslim lands. Understanding this contextual evolution is critical in the effort to find strategies to weaken Al-Qaeda’s ideology.

The foregoing is Article No. 1 (TR416A01) in the **Terrorism Open Source Intelligence Report (TOSIR)**, No. 416, 31 December 2009, prepared by Interaction Systems Incorporated (isincreports@mindspring.com).

[Top of Article](#)

[Article 2 Return to TOSIR Cover Page](#)

2. “Countering the Counter-Terrorists: Senior Jihadis Offer Advice on Security Techniques,” by Abdul Hameed Bakier, **Terrorism Monitor**, Vol. 7, No. 11, 30 April 2009 (<http://www.jamestown.org>). [KBTWLegal, KBTKIntel, KBTZTactics, KBTCInternet] We *quote*:

In a quest to spread security and military knowledge that is vital for successful Salafi-jihadi terror operations, **jihadi Internet forums intermittently release training lessons in all kinds of subjects. This article will examine two types of jihadi security training materials.**

The first training episode, published by Al-Qaeda in the South Arabian Peninsula, tutors jihadis on ways to resist interrogation. The group published three training episodes entitled “Triumph over Interrogators” in [early 2009 in] their monthly e-magazine, Sada al-Malahim.

A second security training episode was prepared by an Ingush jihadi nicknamed Abu Anas of Khacharoy . . . , an Arab field commander operating in Chechnya. This posting discusses intelligence and security techniques in an article entitled

“Security Advice from an Ingush Jihadi.” The material is based on the experiences of Salafi-jihadi fighters operating in the Russian North Caucasus republic of Ingushetia.

[A jihadi perspective on ways to triumph over interrogators]

The anti-interrogation lessons, prepared by an Al-Qaeda operative nicknamed Abdulaziz al-Abini, **discuss two methods of interrogation aimed at eliciting confessions and intelligence from imprisoned jihadis and ways to counter them. The first method is psychological manipulation and the second method is physical torture.** The lesson starts with the psychological methods used by security forces, which begin on day one of imprisonment when the jihadi is restrained with chains as a show of authority. This is typically followed by further manipulative techniques.

Intimidation versus Endearment—This method is applied by two interrogators. One plays the good guy and the other the bad guy. The good guy interrogator will promise to help the jihadi if the latter confesses and provides intelligence on the terror cell. The training warns jihadis not to fall for the false promises of this interrogator. The bad guy interrogator will use obscene language while threatening the jihadi with all kinds of torture. The countermeasure suggested by the training is to simply ignore the interrogators’ threats—easier said than done.

Empathy—Interrogators use empathy, pretending to care for the jihadi’s fate in an attempt to build rapport with the subject. Building rapport achieves short-term and long-term objectives for security forces. The long-term objective is to recruit the jihadi and release him to penetrate the terror cell. **Even though the technique is a very common and crucial instrument in counterterrorism operations, the training fails to explain how the jihadi is supposed to counter this technique.**

Indifference—Leaving the imprisoned jihadi for long intervals without interrogation is another technique used by interrogators when no timely intelligence is required in the given case. In this case, **the jihadi is instructed to pretend to be coping well with prison conditions and spend the time reciting the Holy Qur’an.**

Exaggeration—The interrogators will question the jihadi about a very serious case, implying his involvement, such as a conspiracy to assassinate a head of a state. This technique is designed to manipulate the captive into confessing to a lesser evil and to study his reactions when he is being honest and compare them to his reactions when he lies. To fend off this technique, **the jihadi should answer sarcastically to all allegations. . . .**

Simplify—The interrogators try to convince the jihadi that his case is not serious, unless he keeps denying the charges. The training reminds the jihadi that denying the charges will not exacerbate the case legally.

Wear Out—The jihadi is repeatedly questioned about a single incident.

Insult—Obscene language may be used in the interrogation to break the jihadi’s morale. Interrogators may curse God and religion to shake up the pious jihadi who is ordered by God not to tolerate blasphemy and to try and stop it in any way possible. In this case, the jihadi might think it is **better to confess than to let the blasphemy continue.**

The Bombshell—After long sessions of trivial conversation, the interrogators will **surprise the jihadi with questions related to terror activities, hoping to catch him off guard.** The training relates other “bombshell” techniques from actual experience, such as awakening the suspect and immediately posing questions.

Uncertainty—The training warns the jihadi not to believe allegations that security forces have penetrated the terror cell using one of the amirs ["commanders" or "princes"]. The attempt to cast doubt in the jihadi's mind and weaken his loyalty to his group is an old technique known even to novice jihadis. **The jihadi must have strong faith in the face of the authorities' efforts to dissuade him from his path, such as the Saudi Arabian reeducation and reconciliation prison program.** The training promises separate lessons on countering the rehabilitation program in future issues of [the monthly e-magazine, Sada al-Malahim].

Entrapment—Interrogators will ask questions that sound trivial, such as the time of a particular terror cell meeting, the kind of drinks served in the meeting, and details of the rendezvous place. **The training warns that the answers to these seemingly irrelevant questions will be used on another imprisoned cell member to convince him security forces have comprehensive intelligence about the cell.** Captured jihadis are instructed to give short “yes” or “no” answers to such inquiries because elaboration leads to the disclosure of sensitive intelligence.

Polygraph—The training briefly explains polygraph technology. **The instructions to counter the polygraph reveals that the jihadis do not fully understand the technology or do not train their operatives to deceive the polygraph by using Yoga techniques,** as do some other insurgent groups.

The training warns that interrogators can persist in breaking the suspect if they are convinced the suspect is holding back crucial intelligence on activities that might jeopardize human lives. **Interrogators will also use all possible means to get a conviction if they believe the jihadi would resume terror activities when released.**

[A jihadi perspective on coping with physical duress and using cover stories]

The second part of the training discusses physical duress methods allegedly used by all security forces against Salafi-jihadis. The training describes different torture techniques and urges jihadis to endure pain for the sake of God, who will reward them in heaven.

The training session puts emphasis on the importance of cover stories. Examples are given of the repercussions of bad cover stories in real encounters with security forces. Finally, **the lessons sum up counter-interrogation techniques by instructing jihadis to preplan for interrogation in order to minimize the effects of interrogation on future jihad operations.** Different cover stories should be devised for each and every terror plot. **Tolerance, sarcasm, and indifference will wear out the interrogator,** resulting in a “triumph over the interrogators.”

No matter how thorough and experienced the jihadis are in anti-interrogation, **the fact remains that human psychology differs from person to person. Jihadi tactics have failed to address the wide range of psychological methods researched and adopted**

by security forces. For example, there is no mention in the training of the four different psychological categories interrogators use to try to identify the suspect at the beginning of each interrogation.

[Security advice from the Ingush jihadi nicknamed Abu Anas of Khacharoy]

This security posting, supposedly prepared by an Ingush Salafi-jihadi [with the nickname of Abu Anas of Khacharoy], **aims to educate fellow mujahideen about necessary safety procedures from lessons learned in the North Caucasus jihad.** The author warns that security agents continuously inquire about ways to join jihad through Internet forums, hoping to deceive and identify jihadis involved in trafficking mujahideen. Jihadi candidates must maintain safety requirements and take precautions to avoid capture.

Although jihad has been waged for many years in the Caucasus, very few Muslims were able to safely travel to the Caucasus and join in, says Abu Anas. Additionally, negligence and incompetent security practices, even by experienced jihadis, have led to arrests which decreased the already modest number of mujahideen active in the Caucasus. **Jihad in regions heavily controlled by security forces requires extra precautions and good cover stories capable of disguising even the intention of joining jihad. To hide these intentions, the author suggests would-be jihadis take the following measures:**

- **The elimination of all religious aspects of appearance**, such as the beard and the traditional Salafi dress code.
- **Avoid frequenting mosques.** Mosques are closely monitored by security services.
- **Avoid discussions about jihad with unreliable Muslims who don't believe in the pillar of jihad.**
- **Allow women to take off their head covers to disguise religious commitment.** Abu Anas claims there is a fatwa authorizing this measure.

[Abu Anas: Jihadis must use safe communications, severely punish those who are sloppy]

To stress the importance of eliminating religious aspects of the jihadi's appearance, Abu Anas says Russian secret services arrested, by chance, an active jihadi among many bearded men in connection with a botched assassination attempt on the pro-Russian president of Chechnya.

Abu Anas warns that the Internet is a very valuable source of information for secret services, blaming jihadis for carelessly posting pictures and video clips pertinent to jihad. He offers the example of a policeman's son who made a jihadi-style video while holding his father's state-issued weapon. Security services were able to identify the serial number on the gun and arrest the would-be jihadi. **Abu Anas cautions against trusting relatives in the security services**

The release of pictures and videos on the false assumption that the jihadis in these graphics are already known to the secret services limits the chance of those jihadis conducting any kind of clandestine operation, such as collecting intelligence on a possible target. **Despite Abu Anas’ warnings, jihadis in the Caucasus keep posting their pictures on the Internet, apparently in an attempt to solicit donations from jihad supporters.**

Insecure communications methods, such as land lines, mobile phones, and the Internet, are a major factor in compromising jihad activities. For the security services, this is the fastest and easiest way to uncover jihadi intentions. Secret services eavesdrop on what the jihadi says and analyze what he writes.

Therefore, **jihadis must turn off mobile phones in secret meetings and throw away SIM [Subscriber Identity Module] cards if phone calls suddenly disconnect.** Jihadis who release audio statements through any means must realize that their voiceprint is saved in the electromagnetic database of the secret services for future auto-tracking.

Abu Anas says there are **no secure telephones—80 to 90 percent of successful security operations against jihadis are, at least in part, the result of intelligence collected through technical means.** Hence, jihadis should train on safe communications and severely punish those who are sloppy in these areas.

[Security precautions recommended by Abu Anas]

Finally, [the Ingush jihadi nicknamed Abu Anas of Khacharoy] recommends the following security precautions:

- **Avoid Russian servers when using Internet communications. All Russian police forces have authorized access to any e-mail.**
- **Insurgent groups must immediately expel any mujahid who fails to perform his duties in a secure fashion.**
- **A bad mobile connection in a place that usually has good reception indicates the secret services are listening in on the call. Evacuate the area immediately and dispose of the SIM card. SIM cards are the first things to be checked by secret services when a jihadi is arrested.**

Although more advanced jihadi training materials have been made available on the Internet, the “General Security Advice” prepared by the Ingush jihadi was posted in almost all Salafi-jihadi forums and blogs to depict a united Salafi-jihadi global front. . . .

The foregoing is Article No. 2 (TR416A02) in the Terrorism Open Source Intelligence Report (TOSIR), No. 416, 31 December 2009, prepared by Interaction Systems Incorporated (isinreports@mindspring.com).

[Top of Article](#)

Article 3 [Return to TOSIR Cover Page](#)

3. “**Crime and Terrorism**,” by Colonel Robert B. Killebrew, U.S. Army (Ret.), Small Wars Journal, 2009 (<http://smallwarsjournal.com/blog/2009/11/crime-and-terrorism>). [KBTTCrime,

KBTWFinances, KBTTNarcotics, KBTWAmalgam, KBTHStateLocal] Robert B. Killebrew is a senior fellow at the Center for a New American Security. We *quote*:

The United States has been at war in Iraq and Afghanistan now for eight years, and a great deal of our best thinking and most focused military development has quite rightly gone into fighting those two conflicts. We have built an effective counterinsurgency doctrine, we have re-equipped and re-re-equipped our forces, and we have performed built huge bases of experience in dealing with Islamic insurgent and terror organizations. **This is as it should be—Secretary of Defense Robert Gates’ admonition to “win the war you’re in” is right on target.**

In those eight years, though, **as we have focused on the wars we’re in, there have been some profound changes in the structure of global terrorism, particularly with regard to the relationship between terrorist movements and international crime.** According to a panel of experts at a recent conference sponsored by the Center for a New American Security, **terrorism and crime have now merged, to such an extent that all terrorist movements—all of them—have become partly criminal organizations** to fund their operations, expand their reach—and incidentally **make the people on top extremely rich, while lower-level zealots continue to be recruited for suicide missions.**

[**Terrorism only subset of illegality, aggression against underpinnings of civil society itself**]

In recent appearance before Congress, **one field-experienced Drug Enforcement Administration (DEA) veteran said:** “As we witness the continued evolution of the Taliban, we must also recognize we are witnessing **the evolution of twenty-first century global organized crime.** It is becoming more and more difficult to distinguish the terrorist from the cartel member, because they are operationally and organizationally interbreeding and morphing into one and the same. **The indisputable convergence of terrorism and international drug trafficking is playing out before our very eyes in Afghanistan, and in many other places around the globe.”**

It is sometimes difficult for traditionally-trained military professionals and national security types to recognize crime as a national security threat—at least, it has been for me. But a glance at the **drug wars in Mexico** (and along our border) should make it clear that insurgents and counterinsurgency now takes place in a criminal, as well as sometimes an ideological or political, context. **Worse, the scope of the estimated 1.5 trillion dollars in illicit money being raised around the world, being infused in the global monetary stream, and manipulated by criminals, threatens to undermine the stability of the international order itself, striking at financial and banking systems and undermining legal and political authority in legitimate states.**

Against such deterioration, **terrorism is only a subset of a larger problem of illegality and aggression against the underpinnings of civil society itself, as we see in Mexico and other countries in which criminals have acquired firepower equal to the state.**

[**Afghanistan, Iraq have nudged U.S. strategy and policy toward more integrated solutions**]

How did this happen? Trafficking in illegal drugs has been a challenge worldwide for generations. **But the ripple effects of the collapse of the Soviet Union in the 1980s with its stockpiles of weaponry, the consequent migration of peoples, the**

communications revolution, and easy access to transportation all came together to allow criminals to expand internationally. Although illegal drugs still comprise the most rewarding cash crop for the black economy, other criminal activity, particularly human trafficking and weapons sales, have also expanded.

As a consequence, **international criminal organizations have gone global**; the Revolutionary Armed Forces of Colombia, for example, has agents in West Africa, just as Lebanon's Hezbollah operates in South America (as does the Iranian Revolutionary Guard). More ominously, **some legitimate states now engage in drug production, trafficking, and other illicit commerce, and protect both the trade and its perpetrators behind the state's cloak of legality and international standing—North Korea, Iran, and Venezuela do so,** among others. The **narco-state** has emerged, which vastly complicates the challenge of fighting both crime and terrorism.

Fortunately for us, **our recent experience in Afghanistan and Iraq has begun to nudge American strategy and policy toward more integrated solutions than purely military or purely diplomatic choices,** and we have begun to rebuild the civilian institutions with which we engage the world. **U.S. law enforcement agencies, notably the FBI and DEA, are heavily committed globally in partnership with foreign law enforcement organizations. Domestically, the United States has fairly professional local police forces, generally incorruptible local governments, and efficient and honest courts—**the civic backbone needed to resist assault by Latino gangs like MS-13 and the cartels that are presently moving across the border into the United States.

[Proper answer to challenge of international crime is effective civil institutions]

Here are some early steps that American policymakers, diplomats, and security experts can take.

First, we need to recognize the scope of the problem, and see terrorism, where appropriate, as one arm of international crime. In fact, the emphasis on crimefighting is already reflected inside and outside our two combat theaters, where the leading tools in fighting criminal terrorists are legal investigations, indictments, extradition, and prosecution in U.S. courts. **In many ways, we are returning to pre-9/11 policies to treating terrorists as what they really are and what we ultimately want them to be seen as—criminals who should be brought to justice.**

Doing so not only reaffirms the relationship of international law to terrorists captured in domestic settings—a problem that has plagued the United States since the establishment of Guantanamo—but it also buttresses the authority of legal systems worldwide, which is a fundamental and necessary strategy in fighting a global crime wave. The United States must explicitly reaffirm its commitment to international law and the sovereignty of individual states, and adopt policies to support its position.

Second, we and our allies must continue to reinforce and police the international economic system, to include identification of “black” accounts and banks that likely support illegal or extremist activity. While the United States was vigorously involved in doing so in the aftermath of 9/11, **the passage of time, new administration priorities, and the global financial crisis have apparently resulted in a slowdown of U.S. efforts to seek out and attack criminal misuse of the financial system.**

Third, it's apparent even without the complication of international crime that a major and consistent U.S. strategy is necessary to help our allies rebuild local security forces, police, courts, and legal systems to withstand attempts by insurgents to destabilize their societies and governments. The merger of crime and terrorism means that insurgents will have access to virtually unlimited cash and that widespread attacks on the fabric of civil life—bribes, extortion, kidnapping, murder—have already become common fare in insurgencies.

As the proper answer to this kind of challenge is effective civil institutions, including uncorrupted and efficient police, the United States must be capable of effectively and discretely helping our allies when asked, without opening our friends up to charges of “selling out” their countries’ interests to the Americans. Doing so will mean building on our successes and learning from our failures in rebuilding civil institutions in Iraq and Afghanistan; the continued rebuilding (and in some cases redesign) of our civilian arms of foreign policy, a revamping of our security assistance programs, and tighter integration of our military and diplomatic capabilities. **We have the vision—we just need to do it.**

Finally, **the United States must more effectively bridge the gap between foreign and domestic security policies; criminals and extremists aren't deterred by national borders, and our own law enforcement agencies in the United States—especially local cops on the beat—should have at least the same capability to communicate across boundaries and within organizations as the crooks do. Reinforcing our front-line civic institutions that keep order—police, courts, local governments—has not normally been a priority for national government in our federal system, but it's necessary today as a matter of national security.**

[Explosion of illicit economy and merger of crime and terrorism an imminent challenge]

The foregoing is a first, and almost superficial, overview of developments in the “black” world in roughly the past decade. While our armed forces have been occupied with wars overseas, and our attention has properly focused on them, other developments have changed the nature of some threats to our national security. There are still plenty of more traditional challenges; Russia continues to push back against the West; the Iranians threaten to build nuclear weapons. (Both states, though, either shelter criminal activity or engage in it as state policy.)

But the explosion of the illicit economy, the merger of crime and terrorism, and their reach inside our borders, have added a new and possibly more imminent challenge to our safety—not only at the national level, but on our streets.

The foregoing is Article No. 3 (TR416A03) in the [Terrorism Open Source Intelligence Report](#) (TOSIR), No. 416, 31 December 2009, prepared by Interaction Systems Incorporated (isinreports@mindspring.com).

[Top of Article](#)

Article 4 [Return to TOSIR Cover Page](#)

4. “Securing the Information Highway: How to Enhance the United States’ Electronic Defenses,” by Wesley K. Clark and Peter L. Levin, [Foreign Affairs](#), November-December 2009. [KBTCCyber] Wesley K. Clark, a retired four-star U.S. Army general, was Supreme

Commander of NATO from 1997 to 2000, led the alliance of military forces in the 1999 Kosovo war, and is a senior fellow at UCLA's Ron Burkle Center for International Relations. Peter L. Levin was the founding CEO of the cybersecurity company DAFCA and is now Chief Technology Officer and Senior Adviser to the Secretary at the Department of Veterans Affairs. We *quote* from <http://www.foreignaffairs.com/articles/65499/wesley-k-clark-and-peter-l-levin/securing-the-information-highway#>:

During the 4 July holiday weekend, the latest in a series of cyberattacks was launched against popular government Websites in the United States and South Korea, effectively shutting them down for several hours. It is unlikely that the real culprits will ever be identified or caught. Most disturbing, their limited success **may embolden future hackers to attack critical infrastructure**, such as power generators or air traffic control systems, with devastating consequences for the U.S. economy and national security.

[U.S. has limited ability to detect stolen data—physical hardware increasingly insecure]

As Defense Secretary Robert Gates wrote earlier this year in these pages, **“The United States cannot kill or capture its way to victory” in the conflicts of the future. When it comes to cybersecurity, Washington faces an uphill battle.** And as a recent Center for Strategic and International Studies report put it, **“It is a battle we are losing.”**

There is no form of military combat more irregular than an electronic attack: it is extremely cheap, is very fast, can be carried out anonymously, and can disrupt or deny critical services precisely at the moment of maximum peril. Everything about the subtlety, complexity, and effectiveness of the assaults already inflicted on the United States' electronic defenses indicates that **other nations have thought carefully about this form of combat.** Disturbingly, **they seem to understand the vulnerabilities of the United States' network infrastructure better than many Americans do.**

It is tempting for policymakers to view cyberwarfare as an abstract future threat. After all, **the national security establishment understands traditional military threats much better than it does virtual enemies.** The problem is that an electronic attack can be large, widespread, and sudden—far beyond the capabilities of conventional predictive models to anticipate. **The United States is already engaged in low-intensity cyberconflicts, characterized by aggressive enemy efforts to collect intelligence** on the country's weapons, electrical grid, traffic control system, and even its financial markets.

Fortunately, **the Obama administration recognizes that the United States is utterly dependent on Internet-based systems and that its information assets are therefore precariously exposed.** Accordingly, it has made electronic network security a crucial defense priority. But networks are only the tip of the iceberg. **Not only does Washington have a limited ability to detect when data has been pilfered, but the physical hardware components that undergird the United States' information highway are becoming increasingly insecure.**

[Russia has already perpetrated denial-of-service attacks against entire countries]

In 2007, there were almost 44,000 reported incidents of malicious cyberactivity—one-third more than the previous year and more than **ten times as many as in 2001.**

Every day, millions of automated scans originating from foreign sources search U.S. computers for unprotected communications ports—the built-in channels found in even the most inexpensive personal computers. **For electronically advanced adversaries, the United States' information technology (IT) infrastructure is an easy target.**

In 2004, for example, **the design of the National Aeronautics and Space Administration's Mars Reconnaissance Orbiter, including details of its propulsion and guidance systems, was discovered on inadequately protected "zombie" computer servers in South Korea.** Mimicking the tactics of money launderers, hackers had downloaded them there in order to pilfer the data from a seemingly legitimate source. **Breaches of cybersecurity and data theft have plagued other U.S. agencies as well:** in 2006, between ten and 20 terabytes of data—equivalent to the contents of approximately 100 laptop hard drives—were illegally downloaded from the Pentagon's non-classified network, and the State Department suffered similarly large losses the same year.

Russia has already perpetrated denial-of-service attacks against entire countries, including Estonia, in the spring of 2007 an attack that blocked the Websites of several banks and the prime minister's Website—**and Georgia,** during the war of August 2008. In fact, shortly before the violence erupted, Georgia's government claimed that a number of state computers had been commandeered by Russian hackers and that the Georgian ministry of foreign affairs had been forced to relocate its Website to Blogger, a free service run by Google.

[Cyberattacks are inherently attractive to adversaries large and small]

The emergence of so-called peer-to-peer (P2P) networks poses yet another threat. These networks are temporary on-demand connections that are terminated once the data service has been provided or the requested content delivered, much like a telephone call. Some popular P2P services, such as Napster and BitTorrent, have raised a host of piracy and copyright infringement issues, mostly because of recreational abuse.

From a security perspective, **P2P networks offer an easy way to disguise illegitimate payloads** (the content carried in digital packets); through the use of sophisticated protocols, **they can divert network traffic to arbitrary ports. Data containing everything from music to financial transactions or weapons designs can be diverted to lanes that are created for a few milliseconds and then disappear without a trace,** posing a crippling challenge to Washington's ability to monitor Internet traffic. Estimates vary, but **P2P may consume as much as 60 percent of the Internet's bandwidth; no one knows how much of this traffic is legitimate, how much violates copyright laws, and how much is a threat to national security. . . .**

The price of perpetrating a cyberattack is just a fraction of the cost of the economic and physical damage such an attack can produce. **Because they are inexpensive to plan and execute, and because there is no immediate physical danger to the perpetrators, cyberattacks are inherently attractive to adversaries large and small.** Indeed, **for the most isolated (and therefore resource-deprived) actors, remote, network-borne disruptions of critical national infrastructure**—terrestrial and airborne traffic, energy generation and distribution, water- and wastewater-treatment facilities, all manner of electronic communication, and, of course, the highly automated U.S. financial system—**may be their primary means of aggression. . . .**

[Americans' false sense of security most dangerous advantage for U.S. adversaries]

A hardware breach is more difficult to detect and much more difficult to defend against than a network or software intrusion. There are two primary challenges when it comes to enhancing security in chips: ensuring their authenticity (because designs can be copied) **and detecting malevolent function inside the device** (because designs can be changed). One could easily imagine a kill switch disabling the fire-control logic inside a missile once it had been armed or its guidance system had been activated, effectively disabling the tactical attack capability of a fighter jet.

Inauthentic parts are also a threat. In January 2008, for example, the FBI reported that 3,600 counterfeit Cisco network components were discovered inside U.S. defense and power systems. **As many as five percent of all commercially available chips are not genuine—having been made with inferior materials that do not stand up under extreme conditions**, such as high temperatures or high speeds.

Even well-intentioned security efforts cannot provide ironclad safety. With only \$10,000 worth of off-the-shelf parts, a research group led by Christof Paar at Ruhr-Universität Bochum, in Germany, **built a code-breaking machine that was able to exploit a hardware vulnerability and, within ten seconds, crack the encryption scheme of the electronic passport chip in European Union passports.** This breach could have exposed sensitive personal information to financial criminals and passport counterfeiters. The original design of the passport chip was not fundamentally flawed, but it was inadequately hardened, and no software upgrade could solve the problem.

Adversaries planning cyberattacks on the United States enjoy two other advantages. The first, and most dangerous, is Americans' false sense of security: the self-delusion that since nothing terrible has happened to the country's IT infrastructure, nothing will. Such thinking, and the fact that so few scientists are focused on the problem, undercuts the United States' ability to respond to this threat. **Overcoming a complacent mentality will be as difficult a challenge as actually allocating the resources for genuine hardware assurance. Second, the passage of time will allow adversaries and cybercriminals to optimize the stealth and destructiveness of their weapons;** the longer the U.S. government waits, the more devastating the eventual assault is likely to be.

[Core design principle of any multifaceted system is that diversity fortifies defenses]

Seeking to completely obliterate the threats of electronic infiltration, data theft, and hardware sabotage is neither cost-effective nor technically feasible; **the best the United States can achieve is sensible risk management. Washington must develop an integrated strategy that addresses everything from the sprawling communications network to the individual chips inside computers.**

The U.S. government must begin by diversifying the country's digital infrastructure; in the virtual world, just as in a natural habitat, a diversity of species offers the best chance for an ecosystem's survival in the event of an outside invasion. **In the early years of the Internet, practically all institutions mandated an electronically monocultural forest of computers, storage devices, and networks in order to keep maintenance costs down.**

The resulting predominance of two or three operating systems and just a few basic hardware architectures has left the United States' electronic infrastructure vulnerable. As a result, simple viruses injected into the network with specific targets—such as an apparently normal and well-trusted Website that has actually been infiltrated—have caused billions of dollars in lost productivity and economic activity.

Recently, national intelligence authorities mandated a reduction in the number of government Internet access points in order to better control and monitor them. This sounds attractive in principle. The problem, of course, is that **bundling the channels in order to better inspect them limits the range of possible responses to future crises and therefore increases the likelihood of a catastrophic breakdown.**

Such “stiff” systems are not resilient because they are not diverse. By contrast, **the core design principle of any multifaceted system is that diversity fortifies defenses.** By imposing homogeneity onto the United States' computing infrastructure, generations of public- and private-sector systems operators have—in an attempt to keep costs down and increase control—exposed the country to a potential catastrophe. **Rethinking Washington's approach to cybersecurity will require rebalancing fixed systems with dynamic, responsive infrastructure.**

In addition to building diverse, resilient IT infrastructure, it is crucial to secure the supply chain for hardware. This is a politically delicate issue that pits pro-trade politicians against national security hawks. Since most of the billions of chips that comprise the global information infrastructure are produced in unsecured facilities outside the United States, national security authorities are especially sensitive about the possibility of sabotage.

Some observers have pointed to the Clinton-era Information Technology Management Reform Act as a leaky crack in the levee of secure hardware infrastructure because it explicitly encouraged the acquisition of foreign-made parts. They are wrong. In fact, **streamlining procurement of IT components is in no way related to the integrity of the components themselves; how the government purchases components is unrelated to what is actually delivered, tested, and deployed.**

[U.S. would be more secure following more “open source” approach to information sharing]

Moreover, **the enormous cost of maintaining a parallel domestic production capability to match the tremendous manufacturing advances of the private sector abroad would never pass muster in even the most hawkish appropriations review; such dedicated production facilities would also make an easy target for sabotage or direct attacks.** A disruption in the supply chain would exact an incalculable price, not least in terms of the United States' defensive readiness, and would violate the principle of having a layered, diversified response. It makes sense now—just as it made sense during the Clinton years—to purchase components, even those made offshore. **The problem is not foreign sourcing; it is ensuring that foreign-made products are authentic and secure.**

None of this will require a fundamental change in the way computer networks are currently configured and deployed. Because hardware itself can now be reconfigured—and is therefore adaptable—electronic defenses within actual devices can

be augmented without domestic chip designers' revealing more than they already do to the foreign manufacturers who actually produce the chips.

Of course, **adversaries could build in hardware deficiencies during production that could hurt the United States later. But there are some very elegant ways to detect those deficiencies without the adversaries' knowing that Washington is watching.** Promising strategies in the near term, such as embedding compact authentication codes directly into devices and configuring anti-tamper safeguards after the devices are produced, will enhance protection by tightening control of the supply chain and making the hardware more "self-aware."

The Bush administration's classified Comprehensive National Cyber Security Initiative, which led to a reported commitment of \$30 billion by 2015 to bolster electronic defenses and **which the Obama administration is expected to support, is a solid first step toward managing the risk.**

Unfortunately, **much of the relevant information**—such as the Defense Advanced Research Projects Agency's TRUST in Integrated Circuits program—**is classified. Confidentiality will not necessarily help** ensure that the nation's information assets are well protected or that its cyberdefense resources are well deployed. In fact, **because many of the best-trained and most creative experts work in the private sector, blanket secrecy will limit the government's ability to attract new innovations that could serve the public interest. Washington would be better off following a more "open source" approach to information sharing.**

The cybersecurity threat is real. Adversaries can target networks, application software, operating systems, and even the ubiquitous silicon chips inside computers, which are the bedrock of the United States' public and private infrastructure. **All evidence indicates that the country's defenses are already being pounded, and the need to extend protection from computer networks and software to computer hardware is urgent.**

The U.S. government can no longer afford to ignore the threat from computer-savvy rivals or technologically advanced terrorist groups, because the consequences of a major breach would be catastrophic.

The foregoing is Article No. 4 (TR416A04) in the [Terrorism Open Source Intelligence Report \(TOSIR\)](#), No. 416, 31 December 2009, prepared by Interaction Systems Incorporated (isincreports@mindspring.com).

[Top of Article](#)

[Return to TOSIR Cover Page](#)