"Air Education and Training Command – Develop America's Airmen Today...For Tomorrow"
AIR UNIVERSITY
THE INTELLECTUAL AND LEADERSHIP CENTER OF THE AIR FORCE
We make a difference, one student at a time.
NATIONAL SPACE STUDIES CENTER
Air University, Maxwell AFB, Montgomery AL

Public Enemies In Cyberspace

By Mark Stout

Note: this article originally appeared in the 9 July 2009 edition of Air University's The Wright Stuff.

The Bryan Burrough best-seller *Public Enemies, America's Greatest Crime Wave and the Birth of the FBI, 1933-1934*, is a captivating and transcendent historical read with a number of thought-provoking implications that juxtapose with today's cyberspace environment. The book examines some of that era's best-known criminals and their activities--mainly bank robbery, grand-theft, and kidnapping--and the government's emergent responses in countering their crimes. Thematically, major analogies that parallel today's cyberspace environment include the concept of criminal sanctuary (to include anonymity and non-attribution), problems with jurisdiction and the law, weaknesses in self-defense and protection, and a glaring need for effective and efficient government responses to criminal events.

St. Paul, Minnesota was a hot-bed of criminal activity in the early 1930s due in part to a corrupt law enforcement community. This setting allowed criminals to purchase security within St. Paul as well as obtain insider-knowledge of what honest, uncorrupted police were thinking and doing. While these compromised insiders were largely interested in increasing their own wealth and power, their actions had secondary and tertiary effects that not only endangered public safety but also created a physical environment that encouraged criminals to retreat to St. Paul in relative or even complete anonymity, providing them a sanctuary for planning, fencing, and recruiting activities.

Today, we have an ill-defined frontier called cyberspace with security for this environment provided, not by altruistic men of principle, but by countries and individuals with interests in increasing their power or "for-profit" companies, whose main purpose is increasing their own wealth and market share. Parallels to the *Public Enemies* era run rampant and include the ability of cyber criminals to operate with relative anonymity, conducting unattributable attacks on American cyber systems, to include those associated with business, utilities, and even the U.S. military. Foreign military intelligence organizations, industry, criminal hackers, insiders, and often, a combination of the four are increasingly engaged in these attacks.

The attacks themselves are likely to be accomplished from and certainly through off-shore sanctuaries, to include physical infrastructure, using systems – some even based in the United States – that are not as concerned about the activities they are harboring as they are with gaining the upper hand or improving the bottom line. While many attacks can be traced back to particular origins outside our borders, those countries, when caught, hide behind a fig-leaf of deniability by blaming the attacks on non-sanctioned and uncontrolled actors within their borders. For example, although not clearly understood how, profligate Chinese hackers somehow manage to escape national-level detection despite the much-seeing electronic-eyes associated with the Great Firewall of China. Cybercrime and security intrusions emanating from Russia are similar. With the exceptions of the cyber attacks in Estonia and Georgia, Russian cyber activity seems to have predominant criminal focus versus a state or industrial emphasis. Just as the criminal safe haven of St. Paul was ignored at a great cost, countries or companies that either sponsor or look the other way with regard to providing cyberspace crime and sanctuary will likewise find the threats generated within their own jurisdiction to be much more expensive and dangerous in the long run.

Before the 1930s, the long arm of the law largely excluded the now-ubiquitous federal government. This, when combined with jurisdictional challenges and immature law, helped create an atmosphere that helped crime flourish. Without a robust federal capability, crime fighting largely fell on city, county, and state efforts, and by the time the crime sprees of the *Public Enemies* era burst forth, with criminals commonly crossing state borders, lawmen would often find themselves lacking the authority to conduct investigations, let alone the authority to compel multi-agency cooperation. The *Public Enemies* were successful in identifying operational gaps and exploiting them. When combined with laws that trailed behind the criminal's initiatives, this put law enforcement in a greatly weakened position. For example, until 1934, it was not even a federal crime to murder a federal agent. As such, state police apprehending criminals in Milwaukee for the Missouri murder of a G-man and two Kansas City policemen would prove to be a delicate exercise in coordinating several highly localized bureaucracies. Today, cyber law--local, federal, and international--greatly trails cyber capabilities. There is little useful international law regarding the cyber domain, and enforcement of these laws is much weaker. This has created a great challenge in securing the domain for legitimate public, business, and national security use. It has also created a worrisome window of opportunity for cyber adversaries to conduct destructive activities against individuals, honest companies and unprepared states.

Self-defense in the 1930s, whether in the form of bank guards or body guards, trailed the initiative manifest in the criminal mind. Without demonstrating any awareness of it, the successful *Public Enemies* criminals planned their attacks using principles of war, such as objective (Interviewer: why do you rob banks? Dillinger: 'cause that's where the money is), offense and mass (having enough men and firepower to overwhelm bank guards, patrons, and police), security (keeping plenty of bogus identification and changing vehicles frequently, with lots and lots of license plates), and maneuver (planned and pre-scripted 'gits' or getaway routes). Today, while industry has marketed cyber defense tools to individual users and corporate and government entities have their own firewalls, these solutions often require implementation by those who are computer security savvy or favor non-information age solutions like blocking USB ports and unplugging from the internet. While some experts say cyber must build on these sorts of defenses, the greater challenge is as simple and substantial as it was generating better security for banks: systems must be created that share what needs to be shared and keep what needs to be kept. Just as Dillinger-era law enforcement needed firepower and bullet-proof vests that overmatched the adversary, today's cyber security requires fully developed and robust offensive cyber operations, including cyber-spying capabilities, counter-cyber efforts, and network and data attackers.

The firepower-deficiencies of early G-men were clearly evident for a time, as FBI agents were not allowed to carry guns. As the challenge of cross-state crime became more menacing and more frequent, additional G-men were brought on board. Author Burrough separated the new hires into two general pots: cowboys and college boys. The cowboys were older, more experienced in law enforcement, less educated on law, and could shoot a gun just fine. Their counterparts were the college boys, who favored the Hoover-ish qualities of diligence, standardization and procedure, and loyalty. The FBI needed all the qualities of both the cowboys and the college boys--and some luck--working in concert, to bring the crime wave of the *Public Enemies* era to a close. Even then, FBI growing pains and blunders were far from uncommon as planning and surveillance efforts were forsaken, evidence was mishandled, and obvious leads were not followed.

Today, defending the cyber domain requires new hires analogous to the cowboys and the college boys: a balanced and highly capable cyber team with a diverse and useful skill set. Whether within the 24th Air Force, the National Security Agency, the recently announced new DoD Cyber Command, or the Department of Homeland Defense, a new culture must be created and developed that features dedicated and organic cyber personnel, contractors, academics, industry, and connections between government agencies working together towards a common objective in a dynamic and often legally ambiguous frontier.

Just as plus-ups in manpower and money were needed for the FBI to mature into an effective crime-fighting tool for a dangerous and expanding crime wave, the DoD's new Cyber Command represents an important step in making the domain safe for current and future cyberspace users. Securing the military part of the cyber domain will be an area of great challenge to DoD, as military services will not want to surrender money, manpower, or mission to the new command. Cooperation between the military and other agencies charged with the same type of mission may prove to be an even greater challenge. Yet these capabilities must be developed, and quickly.

While the cyberspace equivalents of Machine Gun Kelly, Bonnie and Clyde, Baby Face Nelson, Pretty Boy Floyd, the Barkers, and John Dillinger have neither initiated a reign of terror nor yet achieved the infamy associated with those long-ago criminals, it appears that it may also be some time before we witness the emergence of cyber's J. Edgar Hoover, FBI, and local cyber crime-fighters. The opportunity to build cyber defenses against emerging threats is running short on time. Why would they attack? Because that's where the money is.

Mark Stout is a researcher and analyst at Air University's National Space Studies Center and sometimes posts at the blog Songs of Space and Nuclear War. The opinions expressed here are those of the author alone and may not reflect the views and policies of the US Air Force or the Department of Defense.