2015

One Minute to Midnight: Amending the War Powers Resolution to Confront the Coming Cyber Wars

Benjamin L. Monarch
University of Kentucky

Follow this and additional works at: https://uknowledge.uky.edu/klj

Part of the Military, War, and Peace Commons, and the Science and Technology Law Commons

Recommended Citation

Available at: https://uknowledge.uky.edu/klj/vol103/iss3/9

This Note is brought to you for free and open access by the Law Journals at UKnowledge. It has been accepted for inclusion in Kentucky Law Journal by an authorized editor of UKnowledge. For more information, please contact UKnowledges@lsv.uky.edu.
One Minute to Midnight: Amending the War Powers Resolution to Confront the Coming Cyber Wars

Benjamin L. Monarch

INTRODUCTION

In the not-too-distant future, Americans may find their technology-laden lives disrupted by an anonymous and seemingly omnipotent force. On that day, many of our basic assumptions about our way of life will be toppled, and it is possible that our lives may be irreparably altered.

Imagine that an undergraduate needs to pay tuition for his upcoming semester, enters his ATM pin to check that he has the necessary funds, and finds that his account balance is erroneously zero. More alarming, consider a mother who administers a routine antibiotic to her child for an illness, and suddenly the child collapses into anaphylactic shock because the child’s medical records noting the allergy had been manipulated. In another scenario, a businesswoman is flying at 36,000 feet when her airliner enters an inexplicable nosedive and the pilots are denied all manual control of the plane. Envision a grandmother battling hypothermia in her Milwaukee home because the regional power plant has mysteriously exploded in February or that a freight train carrying toxic chemicals has jumped the rails in a rural Alabama community requiring an immediate evacuation of the surrounding area. Even more catastrophic, visualize a deadly E-coli outbreak afflicting millions in Southern California because the sewer lines have flowed into the water supply.

---

1 University of Kentucky College of Law, J.D. Candidate May 2015.
Each of these calamities, among numerous others, can be inflicted through cyberspace. Forty years ago this would not have been possible. However, in the last four decades, our civilization has designed a physical world that functions per the mechanisms of cyberspace. This development has bestowed unimaginable benefits, but it has also created or amplified terrifying risks. The largest of these risks is that cyberspace will become a new battlefield in future wars, and each of the dreadful happenings mentioned above could be a tactic employed in such a war. To mitigate this dark future, rules and procedures must be developed to steer the world through these dangers.

This Note will first address the origin of cyber war and develop a clear description of what cyber war entails. It will then explore the current status of cyber war policy and, ultimately, propose a legislative response to the issues raised by this uncharted battlefield. Specifically, this Note calls for the War Powers Resolution of 1973 ("WPR") to be amended to simultaneously expand presidential authority and enhance congressional oversight over cyber war-making. The idiosyncrasies of cyber conflict necessitate greater flexibility than the Commander-in-Chief is currently allowed under the WPR, but Congress should not issue the President a blank check to launch cyber attacks unilaterally.

I. APPROACHING THE RUBICON: A HISTORY OF CYBERSPACE AND CYBER DESTRUCTION

Understanding how and why cyberspace has created previously inconceivable threats requires looking back to the basic infrastructure of the Internet in its infancy. The forbearers of cyberspace did not, and likely could not, forecast what effect the Internet would have on society, or, moreover, how it would become a medium for criminality and bellicosity. As a consequence, they unwittingly designed a system ripe for such problems.

Establishing when the Internet began is not an easy task because its premise of electronic information transmission is not a modern concept. Abraham Lincoln was the first President to use the telegraph to direct war commands. Then, eighty years later electronic communication was an essential tool of the Allied powers during World War II. These early electronic communications relied upon a system known as circuit switching, which consists of a simple Point A to Point B electronic connection over a dedicated transmission line (e.g., a traditional telephone call). The circuit-switching system, while revolutionary, was too rigid to take full advantage of the data-oriented microprocessor age of the late 1960’s—namely, development of a communications network comprised of multiple users sending information sporadically to different destinations.  

9 Id.
The technology race of the Cold War warranted such a network. In 1969, United States military analysts and various computer scientists, operating under the eventual name Defense Advanced Research Projects Agency ("DARPA"), successfully launched an alternative to the traditional circuit-switching system. The new system relied upon a less strict medium of communication known as "packet switching." Packet switching differed from circuit switching because it grouped data into "packets" rather than one continuous electronic transmission, which allowed data to be parsed and allocated across multiple, perpetually open lines of transmission. In short, the packets made it feasible to create a multi-transmission network of lines in contrast to the single-line transmission circuit-switching system. The developers named the new system Advanced Research Projects Agency Network ("ARPANET"). Though ARPANET was built for Defense Department communication, it initially connected computers at UCLA, Stanford, UC Santa Barbara, and the University of Utah. ARPANET evolved to become what nearly every person on Earth knows as the Internet.

In order to meet the expectations of a packet-switching network, ARPANET had two features that are today the central pillars of the Internet.

First, ARPANET was an open, mostly decentralized domain. In other words, it allowed various users to access it easily, provided numerous points of entry known as "gateways," and lacked central control of the network. This infrastructure envisioned a network used by thousands of scientists exchanging benign, mundane research, not billions of users exchanging anything from flight paths to birthday party pictures to stock purchase orders. Former Special Advisor to the President for Cyber Security Richard Clarke said of ARPANET, "[w]hile the protocols that were developed based on these [factors] allowed for the massive growth in networking and the creation of the Internet as we know it today, they also sowed the seeds for the security problems." Simply put, the Internet's design makes it very easy to use toward destructive ends. However, this same design is what also allows the Internet to enable marvelous achievements. This dichotomy underlies the difficulty of policymaking vis-à-vis the Internet.

---

12 See Hughes, supra note 8.
14 See Copeland, supra note 10.
15 Id.
16 Hughes, supra note 8, at 527.
18 See id. at 81–82.
19 See id. at 82–83.
Secondly, ARPANET intertwined military and civilian communication networks. Initially this posed no security problem. However, with time this feature gave rise to two significant challenges, one legal and the other strategic. First, under this intertwined network, it is difficult to determine when a target is legally military or civilian, which is a necessary determination for proper application of the law of armed conflict. Second, and more worrisome, this feature made military assets vulnerable to cyber attack through a largely uncontrolled network.

Despite ARPANET’s ostensibly utopian beginning, it did not take long before nefarious activity started disrupting the network. The first instances of malware were not destructive in the modern sense but rather designed to annoy and prank other users. The Creeper Virus was an example of annoying malware. Emerging in 1971, the Creeper was the first self-replicating virus, but fortunately it did nothing more than post a message on the infected user’s computer screen reading, “I'm the Creeper: Catch me if you can!” The first antivirus program, the Reaper, eradicated the Creeper.

Once the new millennium was underway, ARPANET had long since become obsolete and the Internet had grown into a global computing network. In the 1990s, the world, particularly the United States, adopted information-technology (“IT”) throughout society. Zealous IT companies of this new era developed an endless array of cost-saving technologies and persuaded both government and private industry to integrate the new systems as rapidly as possible.

IT penetrated nearly every facet of life, corporate profits exploded, and the economy boomed. The IT revolution fundamentally transitioned industrial and governmental operations away from manual control to digital control systems. These developments were so ubiquitous and met with such enthusiasm that manual systems were not only retired, they were also eliminated as emergency replacements. Richard Clarke and Robert Knake likened this situation to Cortés destroying his ships after reaching the New World. That our society entered the new millennium relying almost exclusively on computer-based systems is the crux for why cyberspace, and, by extension, cyber war is a matter of the highest importance.

22 See id.
24 See id.
26 See id.
27 See Gervais, supra note 21, at 17.
28 Id.
29 See CLARKE & KNAKE, supra note 17, at 96.
30 See id. at 96–97.
31 Id. at 96.
32 Id. at 97.
33 Id.
One of the earliest demonstrations of computer-based system vulnerability came when the "Slammer worm" hit the Internet in January 2003.\textsuperscript{34} Slammer exploited a weakness in Microsoft server code.\textsuperscript{35} Doubling every 8.5 seconds, the worm did 90% of its damage within the first ten minutes.\textsuperscript{36} The effects of Slammer were staggering: ATMs in the United States malfunctioned, 911 systems and airline reservations were scrambled, portions of the Internet in South Korea and Japan shut down, phone service in Finland was disrupted,\textsuperscript{37} and it even disabled the safety monitoring system at an Ohio nuclear plant for five hours.\textsuperscript{38} The crippling effects of Slammer served as a wake-up call, but it also gave a glimpse into the astounding power of cyber weaponry.

By the end of the new millennium's first decade, the full range of dangers lurking in cyberspace was apparent. Military and corporate espionage had reached epidemic levels,\textsuperscript{39} and the hacking of financial institution websites was commonplace.\textsuperscript{40} Personal security was equally lacking as phishing emails routinely duped unsuspecting computer users into voluntarily giving out critical personal information, such as social security numbers.\textsuperscript{41}

While troublesome, these cyber attacks were minor compared to the tactics allegedly used in the first instances of cyber war. There is not an official definition of a cyber weapon, but it has been aptly defined as "malicious software that possesses an offensive capability."\textsuperscript{42}

Russia allegedly deployed cyber weaponry freely in the late 2000's, first against Estonia in 2007 and then against Georgia in 2008.\textsuperscript{43} This Note does not seek to substantiate or dispute the veracity of allegations made against Russia. Rather, this Note solely uses these circumstances to demonstrate the idiosyncrasies of cyber weapons in a kinetic war.\textsuperscript{44} The mere fact that these allegations remain unproven underscores a vexing problem unique to cyber war. In cyber war, unlike traditional

\textsuperscript{35} Id.
\textsuperscript{36} Id.
\textsuperscript{37} See id.
\textsuperscript{40} See Michael R. Crittenden, A Call to Arms for Banks, WALL ST. J. (June 14, 2013, 7:51 PM), http://online.wsj.com/news/articles/SB1000142412788733409504578545701557015878.
\textsuperscript{41} See Thomas D. Farrell, Don't Get Speared in the Cyber War, HAW. B.J., Nov. 2011, at 27, 27.
\textsuperscript{43} See CLARKE & KNake, supra note 17, at 14–21.
\textsuperscript{44} Kinetic war is a euphemism for a war involving lethal force. It is a useful term to distinguish between wars involving lethal force and those involving cyber force. See generally Jonathan Allen, 'Kinetic Military Action' or 'Cyber War?', POLITICO (Mar. 24, 2011, 2:39 PM), http://www.politico.com/news/stories/0311/51893.html
war, it is difficult, if not impossible, to ascertain the source of a cyber weapon; this is known as attribution and is readily elusive during cyber war.

The Estonian attack was the result of a political disagreement between Russia and Estonia concerning Estonia’s relocation of a former Soviet Union grave marker.\(^\text{45}\) The weapon of choice was a distributed denial of service ("DDoS"), which essentially floods a network with data to create a sort of cyber paralysis.\(^\text{46}\) For over a week the DDoS attack took down websites of banks, Parliament, the president, and various communication entities.\(^\text{47}\) The Kremlin denied any involvement in the incident and even went so far as to say that it was simply a case of Russian nationalists expressing their frustration over the Estonian grave marker relocation.\(^\text{48}\) Russia’s denial demonstrated one of the overarching concerns of cyber warfare, which is the lack of attribution (identifying the culpable party).\(^\text{49}\)

A year later, Russia instigated a territorial dispute with its neighbor Georgia.\(^\text{50}\) As a prelude to a full land, sea, and air invasion, Russia (allegedly) launched a sophisticated cyber attack against Georgia’s government and media websites.\(^\text{51}\) Like the Estonian attacks, Georgia’s networks were crippled by a wave of DDoS attacks.\(^\text{52}\) This use of cyber attacks was noteworthy because Russia dramatically improved the efficacy of its kinetic war effort by diminishing Georgia’s command and control communications.\(^\text{53}\) Russia again denied any involvement in the attacks, and aside from evidence tracing the initial attacks to Russian servers, the former Soviet Union was never conclusively implicated.\(^\text{54}\)

Similar attacks were directed at the Ukrainian government and NATO in March 2014, contemporaneous with Russia’s Crimean incursion.\(^\text{55}\) Again, Russia denied direct involvement with the attacks.\(^\text{56}\)

The events in Estonia, Georgia, and Ukraine may have shocked the cyber security community, but they likely left no one surprised. However, what alarmed cyber security officials and virtually anyone affiliated with IT and/or the military

\(^{45}\) Id. at 13.


\(^{47}\) See id. at 616 n.61.

\(^{48}\) Id. at 617 n.62.

\(^{49}\) See Carr, supra note 23, at 47.

\(^{50}\) See Raboin, supra note 46, at 619.

\(^{51}\) Id. at 619–20.


\(^{53}\) John Arquilla, *Cyberwar is Already upon Us*, FOREIGN POLICY (Feb. 27, 2012), http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us.

\(^{54}\) Id.


\(^{56}\) Croft & Apps, supra note 55. This Note is not a forum to implicate Russia, but the circumstances discussed herein strongly suggest that kinetic war and cyber war are both common and compatible.
was the emergence of “Stuxnet” in 2010. The strangely named computer worm was a cyber weapon pièce de résistance and a startling leap toward a future where cyber attacks reach beyond the digital realm to destroy objects in the physical world.

In approximately 2006, unconfirmed reports indicate that the United States, in collaboration with Israel, commenced development of a cyber weapon that could target Iran’s nuclear program. Four years later, in the summer of 2010, reports circulated worldwide that a “worm” was infecting computer systems of all levels—the worm was named Stuxnet. Stuxnet infected inestimable systems worldwide but left them unscathed. However, when Stuxnet finally reached its destination, the motor-drive system of the Iranian nuclear centrifuges, it caused the centrifuges to uncontrollably spin at destructively high speeds. In the end, nearly 1,000 centrifuges were demolished and the Iranian nuclear program was stalled for several years.

Neither the United States nor Israel to date has officially acknowledged any involvement in Stuxnet, though numerous leaks suggest both nations played a role in its creation. Furthermore, as was the case with Russia, no concrete evidence has linked either party to the incident (the attribution problem), and Stuxnet is still “alive” in cyberspace. Stuxnet, although highly sophisticated in its programming, is smaller than half a megabyte (or approximately one-fourth the size of a photo taken with an iPhone). The long-term significance of Stuxnet is not immediately obvious, but in terms of cyber warfare, it was a watershed event—some cyber security experts have even likened it to the atomic bombing of Hiroshima. As the

57 See Raboin, supra note 46, at 622.
58 See id. n.78.
60 See id.
63 Nakashima & Warrick, supra note 62.
64 See id.
65 See id.
bombing of Hiroshima ushered in the age of looming nuclear war, so, too, has Stuxnet brought the era of cyber war.

In summation, the preceding 40 years have been technologically stunning, but the advancements have not been risk-free. The confluence of the following four elements makes the perils of cyberspace worthy of serious public debate: the nascent architecture of the Internet allowed for its explosive growth and remarkable power but also made it a potent medium for wrongdoing and war making; the intertwining of civilian and military infrastructure creates challenging legal issues and expanded military targets; a lack of attribution diminishes the risk of retribution thereby encouraging cyber attacks; and the precedent of using cyber weapons offensively in pursuit of military objectives has been established.

II. THIS IS NOT YOUR GRANDDAD’S KIND OF WAR: WHY CYBERSPACE IS DIFFERENT FROM TRADITIONAL BATTLEFIELDS

War has been a tragic feature of our species since time immemorial. Our history is littered with stories of mass casualties and development of terrifyingly powerful weapons. Through all of the atrocities, however, the means of using blood and steel have remained mostly constant until now. Traditional battlefields rely on information as an instrument to deploy kinetic weapons, such as missiles, troops, and submarines. In cyber war, information is the weapon. Adjustment to this evolution has been tentative at best, most notably within international law and specifically the United Nations Charter.

Suppose the United States military seeks to destroy a chemical weapons facility within the sovereign territory of an enemy state. The President can take the traditional approach by ordering the launch of a guided missile to demolish the target. This option will be costly; it will generate endless news reporting and footage, and will likely produce political criticism domestically and internationally—with specific claims that the action violates Article 2(4) of the United Nations Charter. Alternatively, the President could order a Stuxnet-like attack against the facility to destroy it. The latter approach would come at a modest cost, would be anonymous, or at the very least, plausibly deniable; and, under current international law, this approach would not be a violation of state sovereignty or the use of force clause in the U.N. Charter. The only major drawback to using a cyber weapon is that sometimes a missile may be a quicker


69 See Hughes, supra note 8, at 526–27.

70 U.N. Charter art. 2, para. 4 ("All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.").

71 See generally Arimatsu, supra note 42, at 100–02.

solution if the cyber weapon must first be developed. Nonetheless, the incentives currently in place tend to make cyber war preferable to kinetic war.\textsuperscript{73}

Cyber warfare also alters the landscape of geopolitical relations. For example, it remains an open question as to whether a country, like Iran, can respond defensively under Article 51 of the U.N. Charter to the Stuxnet attack.\textsuperscript{74} First, Iran would have to identify the culpable party or parties, which to date remain unconfirmed. Furthermore, assuming a response is legal and Iran confirms the origin of Stuxnet, would the response have to be a proportional cyber attack, or could it be a kinetic attack? The international community has not established rules to answer these questions and govern this scenario.\textsuperscript{75}

In addition to an insufficient international legal regime for cyber war, there is no generally accepted doctrine to keep the peace, such as the Cold War Mutually Assured Destruction ("MAD") doctrine.\textsuperscript{76} Under MAD, the Soviet Union refrained from launching nuclear weapons at the United States simply because the United States would retaliate with its nuclear weapons leaving both nations completely destroyed.\textsuperscript{77} MAD does not apply to cyber warfare for the following reasons: it is exercised instantaneously and without warning, thereby eliminating any opportunity to reciprocate; it lacks attribution; and, it can be conducted by a non-state actor operating beyond the political considerations of most national leaders.\textsuperscript{78}

Concern over cyber war is not without its critics.\textsuperscript{79} Critics correctly state that thus far no humans have been killed by a cyber attack, and no evidence exists to contradict this assertion.\textsuperscript{80} There is also a belief that cyber warfare is preferable to kinetic war, but this attitude is predicated on the belief that cyber warfare can be restricted to cyberspace or will only damage limited, specific targets in the physical world.\textsuperscript{81} These observations are not meritless, but they are backward looking and represent a minority position. In contrast, a recent survey of 352 defense officials

\textsuperscript{73} See CARR, supra note 23 (noting that passive defenses and criminal laws are insufficient to deal with cyber-attacks).

\textsuperscript{74} See Sanger, supra note 68; see also U.N. Charter art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.").


\textsuperscript{76} See Sanger, supra note 68.

\textsuperscript{77} See id.

\textsuperscript{78} See CARR, supra note 23.


\textsuperscript{80} Cyber-Warfare: Hype and Fear, supra note 79.

\textsuperscript{81} Id.
named a cyber attack as the single greatest threat against the United States (terrorism was a distant second). Similar perspectives are found within the United States Congress. House Intelligence Committee Chairman, Representative Mike Rogers, recently said of a cyber attack that it is the "largest national security threat to... face the U.S. that we are not even close to being prepared to handle as a country."83

III. WHERE WE ARE: CURRENT INTERNATIONAL AND DOMESTIC LAW REGARDING CYBERSPACE

On the international level, discussions over how to govern cyberspace and cyber warfare are not new, but they have also not been very constructive.84 Sovereignty has been an essential concept in international law since the Treaty of Westphalia,85 and few concepts complicate cyber warfare discussions more than this one. Because cyberspace transcends national borders on the one hand and has substantial effects within national boundaries on the other hand, it turns the Treaty of Westphalia upside-down.86

For example, if the United States directs a cyber attack against the Cameroonian power grid, and the grid relies on a French Internet Service Provider ("ISP") with critical servers physically located in France, then the attack is not an attack with effects solely in Cameroon. France could claim a violation of its territory, or Cameroon could view France as complicit in the United States intrusion. The default perspective is to view France as a neutral party.87 However, the default position ignores the complexities of cyberspace.88

One of the few international laws to have meaningful effect on cyber warfare is the International Telecommunication Convention ("ITC").89 The ITC requires member states to monitor domestic telecommunication networks and to prevent such networks from being used to transmit information damaging to the State.90

83 Id. (internal quotation marks omitted).
84 See Arimatsu, supra note 42, at 94.
86 See Hughes, supra note 8, at 535–36.
87 See Arie J. Schaap, Cyber Warfare Operations: Development and Use Under International Law, 64 A.F. L. REV. 121, 153 (2009) (discussing the idea that the unauthorized use of another nation's networks may not constitute an unlawful use of force). Schaap highlights that the United Nations Security Council has not viewed intrusions into foreign airspace as unlawful uses of force. Id. These scenarios are comparable to one belligerent nation using a third-party nation's territory as a launch site or pass-thru for military tactics against another belligerent nation.
88 Arimatsu, supra note 42, at 107 (noting that malware can be routed through servers in different countries and, therefore, creates complexities distinct from traditional kinetic attacks).
89 Schaap, supra note 87, at 164 (citing Article 35 of the ITC as an example of the potential regulation of cyber warfare by virtue of prohibiting intentional interference with radio spectrum).
90 Id. at 164–65.
The Obama administration has taken steps to promote international standards governing cyberspace. In its "International Strategy for Cyberspace" of May 2011, the White House voiced support for strengthening network security, promoting freedom of content, and formalizing international standards. The publication provides normative standards for cyberspace strategy and iterates that the United States, like all sovereign states, reserves the right of self-defense against aggressive actions taken in cyberspace. To what extent the White House might invoke this right remains to be seen, but the publication clearly suggests that the Obama administration views cyber aggression as subject to the right of self-defense found in Article 51 of the United Nations Charter.

Despite overtures from the international community and the White House, nothing yet in international law explicitly prohibits/governs the use of cyber weapons. This legal void allows the current cyber arms race to continue unchecked, which serves only to increase the likelihood of cyber warfare in the future.

Domestically there has been more activity to prepare for cyber war, but this activity is far from sufficient. In 2010, the Department of Defense launched the United States Cyber Command to oversee its more than 15,000 networks and more than seven million computer devices. Generally, United States Cyber Command oversees the United States government's entire "mil" domain. As for the United States' "gov" domain for the civilian portion of the federal government, security is under the control of the Department of Homeland Security ("DHS"). The primary DHS office in charge of "gov" security is the Office of Cybersecurity and Communications ("CS&C"). The CS&C has express authority over the "gov" domain, but its role concerning "com" is merely to "collaborate with the private sector." It is the lack of authority over "com" that leaves much of the national network at risk.

92 Id. at 14 (recognizing the inherent right of all sovereign states to self-defense and clarifying that the United States will respond to cyber threats like it would any other threat).
93 Id. at 10 ("Consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace."); see also U.N. Charter art. 51 (providing the inherent right for a Member of the United Nations to act in self-defense in the event of an armed attack against that Member).
94 See Schaap, supra note 87, at 124 (noting that international law does not directly address cyber warfare, although cyber attacks that cause physical damage can violate international laws relating to armed conflict).
95 See Hughes, supra note 8, at 533 (noting that despite the cyber arms race among sovereign states, there remains no international consensus on how to apply the law of war to cyber-attacks).
97 Id.
99 Id.
100 Id.
Congress has floundered for years to produce meaningful cyber security legislation, and even when it has come close, the legislation has been limited to cyber defense, not offense. The main reasons for Congress' ineffectiveness have been first, privacy concerns and, second, burdensome regulation of business. Certainly these are legitimate reservations, as a legislative overhaul of this magnitude would undoubtedly affect nearly every individual or private entity in the nation. However, leaving cyber security policy to the discretion of private industry is not justified considering how integral private industry is to the national security of the United States. Further, failure to adequately secure the Internet is already eroding privacy and burdening economic activity.

As Richard Grelling wrote in his treatise, The Crime, "[W]hen all other means fail, the highest ends of peace are only to be attained by war . . . ." Likewise, an inadequate cyber defense structure is likely to encourage future cyber-attacks. As evidenced by Congress' past efforts to pass cyber security legislation, future attempts will likely be limited to the defense of the national network. Given Congress' inability to pass defense legislation, it is not likely to attempt to pass legislation addressing the power to make cyber offensives.

IV. BRINGING THE WPR INTO THE 21ST CENTURY: AMENDING THE WPR TO PREPARE FOR THE WARS OF THE FUTURE

The United States Constitution is the dominant legal text defining the President's authority over foreign affairs and issues arising under his Commander-in-Chief role. This Note does not question whether provisions enumerated in the United States Constitution are adequate to address the concerns of cyber warfare; rather this author believes they provide sufficient latitude to the President. Second to the Unites States Constitution, the War Powers Resolution of 1973 ("WPR") places restraints upon executive authority. The constitutional basis for the WPR is Congress' power to declare war. In the following paragraphs, this Note will discuss the origin and purpose of the WPR, why the WPR should be applied and amended, and how it should be amended.


102 Alina Seiyukh, House Passes Cybersecurity Bill as Privacy Concerns Linger, REUTERS (Apr. 18, 2013, 9:36 PM), http://www.reuters.com/article/2013/04/19/us-usa-cybersecurity-congress-idUSBRE98H0YU20130419 (reporting that President Obama threatened to veto the Cyber Intelligence Sharing and Protection Act (CISPA) due to privacy concerns).

103 See Fung, supra note 101.


105 U.S. CONST. art. II, § 2, cl. 1–2 (obligating the President to serve as Commander-in-Chief of the armed forces, make Treaties, and appoint Ambassadors).

106 U.S. CONST. art. I, § 8, cl. 11.
Congress passed the WPR in the wake of the Vietnam War and Watergate. Both events spurred Congress to adopt policies meant to weaken the President’s power,107 so Congress strengthened its own war-declaration power by requiring the President keep Congress informed of any war-like activities.108 The major characteristics of the WPR are that it (1) requires the President to notify Congress of the introduction of the United States Armed Forces into hostilities no later than 48-hours after such introduction (“reporting provision”) and (2) that the United States Armed Forces cannot remain engaged in hostilities longer than sixty days without an authorization for military force or a declaration of war from Congress (“authorization/declaration provision”).109

Unsurprisingly, presidents have not embraced the WPR since its passage, but this Note does not analyze the history of presidential dismissiveness toward the WPR.110 For this Note’s purposes, the WPR is taken at face value as the law of the land. However, even if the WPR is considered the reigning law regarding war making in the United States, the WPR as currently written is too antiquated for the unique war making conditions created by cyber warfare.

A. Why Apply and Amend the WPR?

Before assessing the WPR’s inadequacies, a frequent and legitimate concern must be confronted. This issue is whether the WPR must be amended at all in light of Congress’ authority to simply grant limited powers to the President to conduct cyber war. Following the 9/11 terrorist attacks, the United States confronted a new threat, and it was believed that the President needed broad authority to combat the menace.111 Accordingly, Congress passed the Authorization for Use of Military Force (“AUMF”) and the Global War on Terror commenced.112 With the Global War on Terror the United States encountered a new threat, and yet the WPR did not require amendment. So why would an amendment be required to face cyber war? The short answer is that the AUMF and the WPR both envision traditional warfare (soldiers, tanks, jets, and ships). However, cyber war does not, and most likely will not, resemble traditional warfare. This distinction makes the current WPR incongruent with the risks posed by cyber weapons.


108 Id.


110 Brian Hughes, Interactive: Presidents Historically Have Ignored War Powers Resolution, WASH. EXAMINER (Sept. 6, 2013, 12:00 AM), http://washingtonexaminer.com/interactive-presidents-historically-have-ignored-war-powers-resolution/article/2535123.


112 Id.
The central proposition of the WPR is congressional oversight for the use of the United States Armed Forces in hostilities. It is tempting, and strongly arguable, to suggest that the WPR is wholly inapplicable to cyber war because cyber war does not involve the armed forces in the traditional sense. This observation is technically correct, and, accordingly, an AUMF-like authority for cyber war would not seamlessly fall under current WPR language. However, three reasons suggest this is not a basis for dismissing the applicability of the WPR.

First, most conceivable uses of cyber weaponry will involve military personnel at some level, even if they are only sitting behind a keyboard. These individuals will not be in harms-way as in times past, but they will still be executing orders of the Commander-in-Chief against a war target. For this reason, Congress will assert, with some credibility, that the WPR is applicable even in its present form. In fact, Congress has ostensibly stated that it believes the WPR applies to cyber war activities, though specific legislation to this point remains elusive. The mere fact that Congress does, or at least would, assert the relevance of the WPR is sufficient basis not to dismiss its applicability.

Second, there is a public policy issue favoring an amended WPR that goes beyond whether Congress would or would not assert its applicability. If the United States suffered a large-scale cyber attack, then Congress would likely provide an AUMF-like authority to prosecute a cyber war. If such an authority were granted without amending the WPR to encompass the facets of cyber war, then presidents would have an incentive to utilize cyber war as a means of evading WPR reporting provisions. This would diminish transparency and deny the public an opportunity to its government accountable.

Presidents of both political parties have historically resented the WPR as an encroachment upon their power. In fact, the Pentagon has posited that the WPR is not relevant to cyber conflict. The delicate balance of war-making power between the President and Congress ought to be based on a thorough evaluation of the conflict and the policies necessary to quell the conflict. If, however, the President is given one set of WPR-covered war-making authorities (i.e., traditional, kinetic war powers) and another set of non-WPR-covered war-making authorities (i.e., cyber war powers), then the President will tilt toward using cyber war powers more often because they afford greater unilateral decision-making. This scenario creates a perverse incentive that encourages cyber war arbitrarily not necessarily because it is the optimal instrument of offensive war making.

Third, because cyberspace intertwines civilian and military networks and many civilian assets are strategic targets (e.g., the power grid) or instruments of cyber war

113 §§ 1542–1544.
116 See Hughes, supra note 310.
(e.g., civilian ISPs), the President’s cyber war-making needs will envelope the private sector in some form. In accordance with *Youngstown Sheet & Tube Co. v. Sawyer*, the President must have express authority from Congress to expand his Commander-in-Chief authority into the private sector.118 Therefore, Congress should grant express authority to the President using the WPR as the legislative vehicle. If done prospectively, it should improve oversight and regulation of any presidential intrusion into the private sector.

Given the features of cyber war thus far articulated, it is reasonable and necessary for the national security of the United States that Congress grant the President standing authority to intervene in the private sector when executing a cyber offensive or defensive strategy as part of his Commander-in-Chief and foreign affair powers. An example of how this authority may be needed is found in the 2009 Iranian election protests. Iranian election protestors used Twitter (a civilian social network) to coordinate DDoS attacks against the Iranian government.119 Should Twitter be used in a future DDoS attack against the United States military, the President may be compelled to temporarily shut Twitter down. Presently, the WPR fails to foresee a scenario where the President might need to carryout a cyber war strategy via civilian IT. Should this situation arise it would be prudent to have guidelines in place.

By granting the President authority to intervene in the private sector, it is likely that private entities will perform roles akin to military roles. As this would occur outside of the United States Armed Forces and would be analogous to mercenary action, the WPR should be amended to include this scenario under Congressional oversight. Failing to amend the WPR in this regard could encourage the President to circumvent the WPR by relying more readily on civilian assets to prosecute a cyber war. Though both civilian and military assets would likely be required, as a matter of public policy it is preferable to have the President rely mostly on the military, and only the private sector in a legal and transparent manner.

Having such legal authority in place would allow the President to maneuver quickly during an attack. However, this grant should not be without routine congressional oversight, which is why an amended WPR is the most effective legal instrument to adapt to the future of cyber war.

In short, as cyber warfare becomes a more utilized conflict medium, the WPR risks fading into irrelevance as currently written. However, the WPR should not be dispensed with because it does provide useful conceptual architecture for how Congress and the President can share war-making powers. Some scholars have suggested that the current WPR can be loosely interpreted to cover cyber warfare; however, this Note contends that such arguments are a weak substitute for a deliberate amendment process—the issues at stake warrant the thoroughness provided by contemporary legislation.120 Therefore, an amendment designed to make the WPR applicable to twenty-first century war can keep the WPR both

---

119 See CARR, supra note 23, at 144.
120 See Healey & Wilson, supra note 117, at 1, 4–5.
relevant and useful, and can avoid the sort of political charades that often accompany interpretations of antiquated laws.

**B. How to Amend the WPR**

If the WPR is to be amended, it must be changed in ways that reflect the unique qualities of cyber war. The existing WPR provisions should remain in effect for traditional, kinetic war, but new sections pertaining to cyber conflict must be added. By keeping the oversight authority of the WPR, Congress may maintain its precedent of receiving scheduled reports from the President regarding any hostilities—cyber or kinetic. However, an amended WPR can also serve as a tool to expand presidential power in a way that fits the complexities of cyber war.

Currently, Presidents are allowed by law to conduct covert operations (i.e., intelligence gathering) and commence war. The reasons the President has these powers are both constitutional and statutory: first, the Constitution grants the President authority over foreign affairs; and, second, Congress appreciates the national security necessities of allowing the President some flexibility to make snap-decisions. Cyber warfare can fit within either covert or war-making activities, but not without ambiguity. The following hypothetical illustrates this dilemma: The United States decides that elimination of a biological weapons plant in North Korea is in its national security interest. The United States will likely first gather intelligence about the facility, which can be procured covertly by a variety of means, such as human operatives, drones, and computer viruses. If the United States sends human operatives to assess the facility, it falls under covert-actions laws that simply require the President to inform congressional intelligence committees. If, on the other hand, the United States infects the facility computers with a virus designed to relay information, it is unclear whether this is covert activity. Advancing the hypothetical further to a point where the human operative destroys the facility makes the scenario more like a war action, which could trigger the WPR. However, if the same virus is used to destroy the facility, like Stuxnet did, would it be an act of war, a covert operation, or something different?

The distinction between the operative and the virus may not be apparent at first, but consider a third scenario where the operative that assesses the facility also installs a remote-detonated explosive and then leaves the site. The explosive can now remain undetonated until some future date—perhaps years later. For practical purposes, this is how cyber weapons can operate. To pose a latent yet instantaneous

---

123 U.S. Const. art. II, § 2, cl.2.
125 See Dycus, supra note 122, at 158–60.
risk makes the covert versus war making distinctions irrelevant and as a consequence makes applicability of the current WPR very unclear.

Accordingly, the WPR should be amended to define cyber war hostilities as those that are likely to have a kinetic effect (i.e. destruction or disruption of a physical structure or device) in the imminent future. When war, either cyber or kinetic, is foreseeable Presidential authority should be at its apex. Allowing Congress the option to obstruct latent tactics on the basis that they are hostilities under the WPR would render Presidential authority on cyber offense mostly toothless in the eyes of an enemy. This standard would allow the President to install offensive cyber weapons without Congressional intrusion into Commander-in-Chief decisions but would not allow the President to activate said weapons without triggering application of the WPR reporting provision. Analogous to a kinetic war scenario, this standard would allow the President to have an explosive installed without concern for the WPR, but once the decision is made to detonate the device, the WPR would become applicable. An amended WPR would, through the legislative process, introduce important political considerations in the president’s use of latent cyber weapons.

The purpose of focusing on the decision to activate and not the actual activation is the instantaneous effect of cyber weapons. It would be largely symbolic (i.e., meaningless) to require the President to report to Congress concerning a cyber attack that has already occurred.

Additionally, the authorization/declaration provision of the WPR should be amended to expressly exclude automated cyber weapons. While the statutory grant of expanded war power would be the most substantive amendment to the WPR, other alterations would be warranted as well. Even when war is not foreseeable, there is still a risk that cyber weapons may be deployed against the United States (e.g., a cyber Pearl Harbor). The instantaneous impact of such attacks may require the United States to pre-emptively imbed automated cyber weapons within non-United States networks regardless of whether war is foreseeable. This may seem like science fiction, but a recent leak by Edward Snowden alleges existence of a National Security Agency program—codenamed “MonsterMind”—that serves this exact purpose. Such a program would improve the ability to reciprocate with a self-defense attack (i.e., if China begins disabling the United States electric grid, then a preemptively placed cyber weapon would initiate an automated strike against the Chinese electric grid). This is different

---

126 See 50 U.S.C. § 1544(a) (2012) (requiring, implicitly, the same action for cyber warfare as for traditional forms of warfare).
from the latent cyber weapon discussed in the preceding two paragraphs because the attack would not commence following a decision by the President but, rather, would begin automatically if the United States were attacked. These activities should be reported to congressional intelligence committees and be subject to statutory guidelines, but it would be self-defeating to mandate under the WPR that they be reported to Congress for approval. A latent, automated cyber weapon, though potentially necessary, would be impossible to implement if doing so requires a formal authorization/declaration from Congress. Congress can maintain input over cyber weaponry, even those that are automated, but requiring a pre-emptive authorization/declaration for an automated weapon is unsound and illogical.

Furthermore, this Note strongly advises Congress to shorten the traditional forty-eight hour reporting provision and sixty-day authorization/declaration provision when cyber war is at issue. Through cyber war, the President can cripple an entire country within seconds, which makes a forty-eight hour reporting period moot. Presently, the WPR implicitly assumes a war cannot begin and end within two days, but such a scenario is not improbable when cyber weapons are involved. It would be more consistent with cyber war to require the President to report to Congress within an hour. Likewise, a sixty-day authorization/declaration provision is sensible in a world where the mobilization of troops requires weeks of public, non-clandestine activities. The two-month period allows the public, with Congress as its proxy, to evaluate the merit of the war policy. However, a sixty-day window is ineffective when a cyber-war can begin within seconds following a single keystroke. 129 In matters of cyber war, Congress should consider an authorization/declaration timeframe of no more than twenty-four hours. Traditional wars have, with few exceptions, been measured in years. Cyber war, on the other hand, could conceivably be measured in hours—or even minutes.

As if the aforementioned considerations do not complicate this issue enough, government must not undermine the Internet’s worth by supplanting it as little more than a military and surveillance tool. The Internet has transcended the digital world and become integral to democracy, and, as some have argued, is even a basic human right. 130 The proper role of Congress and the President, therefore, is to protect the Internet and its users, not to limit its value with overbroad controls and intrusions. Even though the threat of cyber war is palpable, the Internet must remain an open network that is at its core a medium for the free flow of information. For this reason, this Note implores a thorough and public debate of the recommendations contained herein. Though military activities will ultimately necessitate secrecy at some level, establishing rules to govern cyber war should begin with an open discussion that educates the public and receives input from the citizenry.

129 See Dycus, supra note 122, at 157–58.
CONCLUSION

The Internet has revolutionized the lives of nearly each person on the planet in unimaginably positive ways. However, the Internet has also created hazards that have the potential to disrupt people's lives in horrific ways. Presently, these vulnerabilities are growing in number and severity, and there are few efforts underway to sufficiently address them. This makes the technologically dependent world extremely helpless in the face of cyber aggression. The most effective way to respond to this risk is a robust defense structure and a credible offense capability.

The Presidency is best suited, both legally and practically, to develop and deploy a cyber war offensive strategy. Cyber weaponry is becoming a common element of traditional war, and it is likely that someday wars may be conducted mostly, if not exclusively, in cyberspace. Failure to prepare for these coming conflicts makes them more likely because they will be easier to execute. Presently, the United States has not formed a legal regime tailored to this threat, but it does have an existing legal architecture in the WPR to guide its development.

For the WPR to stay relevant and useful it must be amended to fit the times; otherwise it will become an artifact of a bygone era. The changes recommended in this Note would expand presidential power to effectively confront cyber war threats, but would also fortify Congress's (and by extension the public's) oversight controls. This balance-of-power objective can be advanced by thoughtfully amending the War Powers Resolution of 1973 to accommodate the perilous new world we are entering.
Since 1913, the Kentucky Law Journal has published scholarly works of general interest to the legal community. The Journal is produced by students of the University of Kentucky College of Law under the direction of a fifteen-person editorial board and with the advice of a faculty member.

We welcome unsolicited submissions. Submissions must be typed double spaced with footnotes. Citations should generally conform to the Bluebook: A Uniform System of Citation (19th ed. 2010); the Chicago Manual of Style (16th ed. 2010) is recommended for non-citation stylistic guidance. The author's résumé or a brief biographical statement should accompany the manuscript. Manuscripts will not be returned unless accompanied by a return envelope and postage. Send all submissions to:

editors@kentuckylawjournal.org

or

Articles Editor
Kentucky Law Journal
University of Kentucky
College of Law
Lexington, KY 40506-0048

Electronic submissions are also accepted through the ExpressO online service.

The editing process will be facilitated by sending articles in Microsoft Word format. Any required graphics should consist of high-resolution black-and-white line art provided as separate eps or tiff files.

Except as otherwise provided, the author of each article in this issue has granted to the Journal a nonexclusive license to publish, reproduce, distribute, and use the article in print or electronic form. The Journal hereby authorizes the reproduction of article(s) to be made for classroom use in a nationally accredited law school, provided that (1) author and journal are identified, and (2) proper notice of copyright is affixed to each copy. The views expressed in the articles, etc., do not necessarily represent the views of the Journal.

Communications of an editorial or business nature may be addressed to Kentucky Law Journal, University of Kentucky, College of Law, Lexington, KY 40506-0048. All notifications of change of address should include old address and new address, including zip code. Please inform us one month in advance to ensure prompt delivery.

Subscription price: $44.00 per year, $11.00 per number. Subscriptions are accepted only on a volume basis, starting with the first issue of the current volume. If subscription is to be discontinued at expiration, notice to that effect should be sent before the receipt of the first issue of the next volume; otherwise, subscriptions will be renewed and sent as usual. Claims for issues not received must be made within one year of publication. Back issues and volumes are available from William S. Hein & Co., Inc., 1285 Main Street, Buffalo, NY 14209-1987.

The Kentucky Law Journal is published quarterly by the College of Law, University of Kentucky, Lexington. Periodicals postage paid at Lexington, Kentucky 40506 and additional offices. POSTMASTER: send address changes to Kentucky Law Journal, University of Kentucky, College of Law, Lexington, KY 40506-0048. ISSN 0023-026X.

Copyright 2015 by University of Kentucky College of Law
ELI CAPILOUTO, President of the University. BS 1971, University of Alabama; DMD 1975, MPH 1985, University of Alabama at Birmingham

CHRISTINE M. RIORDAN, Provost. BTE 1987, Georgia Institute of Technology; MBA 1989, PhD 1995, Georgia State University

DAVID A. BRENNEN, Dean and Professor of Law. BA 1988, Florida Atlantic University; JD 1991, LLM 1994, University of Florida

ADMINISTRATION

KEVIN P. BUCKNAM, Director of Continuing Legal Education. BS 1987, Eastern Kentucky University; JD 1992, California Western School of Law

MELISSA N. HENKE, Director of Legal Research and Writing, Assistant Professor of Legal Research and Writing. BA 1998 University of Kentucky; JD 2001, George Washington University

DIANE KRAFT, Assistant Director of Legal Writing and Director of Academic Success. BA 1986, University of Wisconsin; MA 1996, Indiana University; MA 1998, Indiana University; JD 2006, University of Wisconsin

DOUGLAS C. MICHAEL, Associate Dean of Academic Affairs and Gallion & Baker Professor of Law. AB 1979, Stanford University; MBA 1982, JD 1983, University of California

DANIEL P. MURPHY, Assistant Dean for Administration and Community Engagement. BA 1993, JD 1998, University of Kentucky

SUSAN BYBEE STEELE, Associate Dean of Career Services. BS 1985, JD 1988, University of Kentucky

EMERITUS FACULTY

CAROLYN S. BRATT, Professor of Law (Emeritus 2008). BA 1965, State University of New York at Albany; JD 1974, Syracuse University

ALVIN L. GOLDMAN, Professor of Law (Emeritus 2008). AB 1959, Columbia University; LLB 1962, New York University

THOMAS P. LEWIS, Professor of Law (Emeritus 1997). BA 1954, LLB 1959, University of Kentucky; SJD 1964, Harvard University

JOHN M. ROGERS, Judge, US Court of Appeals for the Sixth Circuit, Thomas P. Lewis Professor of Law (Emeritus 2002). BA 1970, Stanford University; JD 1974, University of Michigan

STEPHEN J. VASEK, JR., Associate Professor of Law (Emeritus 2012). BS, BA 1961, JD 1966, Northwestern University; LLM 1969, Harvard University
ALBERTINA ANTGNINI, Visiting Assistant Professor of Law. BA 2004, Stanford University; JD 2008, Harvard University

RICHARD C. AUSNESS, Everett H. Metcalf, Jr. Professor of Law. BA 1966, JD 1968, University of Florida; LLM 1973, Yale University

SCOTT BAUERIES, Robert G. Lawson Associate Professor of Law. BA 1995, University of West Florida; MEd 2001, University of South Florida; JD 2005, PhD 2008, University of Florida

JENNIFER BIRD-POLAN, James and Mary Lassiter Associate Professor of Law. BA 1999, Penn State University; JD 2007, University of Nebraska

TINA BROOKS, Electronic Services Librarian. BA 2005, University of Northern Iowa; JD 2009, University of Texas

RUTHEFORD B CAMPBELL, JR., Spears-Gilbert Professor of Law. BA 1966, Centre College; JD 1969, University of Kentucky; LLM 1971, Harvard University

MARIANNA JACKSON CLAY, Visiting Assistant Professor of Law. JD 1978, University of Kentucky

ALLISON CONNELLY, Director of the UK Legal Clinic and James and Mary Lassiter Professor of Law. BA 1980, JD 1983, University of Kentucky

MARY J. DAVIS, Stites & Harbison Professor of Law. BA 1979, University of Virginia; JD 1985, Wake Forest University

JAMES M. DONOVAN, Law Library Director and James and Mary Lassiter Associate Professor of Law. BA 1981, University of Tennessee at Chattanooga; MLIS 1989, Louisiana State University; PhD 1994, Tulane University; MA 2000, Louisiana State University; JD 2003, Loyola New Orleans School of Law

JOSHUA A. DOUGLAS, Robert G. Lawson & William H. Fortune Associate Professor of Law. BA 2002; JD 2007, George Washington University

WILLIAM H. FORTUNE, Robert G. Lawson Professor of Law. AB 1961, JD 1964, University of Kentucky

CHRISTOPHER W. FROST, Thomas P. Lewis Professor of Law. BBA 1983, JD 1986, University of Kentucky

EUGENE R. GAETKE, Edward T. Breathitt Professor of Law. BA 1971, JD , University of Minnesota

MARY LOUISE EVERTRE GRAHAM, Senator Wendell H. Ford Professor of Law. BA 1965, JD 1977, University of Texas

Jane GRISÉ, Director of Academic Success, Professor of Legal Writing. BA, JD, University of Wisconsin

ROBERTA M. HARDING, Judge William T. Lafferty Professor of Law. BS 1981, University of San Francisco; JD 1986, Harvard University

KRISTIN J. HAZELWOOD, Assistant Professor of Legal Research and Writing. BA 1996, University of Louisville; JD 1999, Washington and Lee University

MICHAEL P. HEALY, Senator Wendell H. Ford Professor of Law. BA 1978, Williams College; JD 1984, University of Pennsylvania
NICOLE HUBERFELD, H. Wendell Cherry Professor of Law. BA 1995, University of Pennsylvania; JD 1998, Seton Hall Law School

MARK F. KIGHTLINGER, Edward T. Breathitt Associate Professor of Law. BA 1981, Williams College; JD 1988, Yale Law School

ROBERT G. LAWSON, Frost, Brown & Todd Professor of Law. BS 1960, Berea College; JD 1963, University of Kentucky

CORTNEY E. LOLLAR, Assistant Professor of Law. BA 1997, Brown University; JD 2002 New York University

KATHYRN L. MOORE, Ashland-Spears Distinguished Professor of Law. AB 1983, University of Michigan; JD 1988, Cornell University

MELYND A. PRICE, Robert E. Harding, Jr. Associate Professor of Law. BS 1995, Prairie View A & M University; JD 2002, University of Texas

FRANKLIN RUNGE, Faculty Services Librarian. BA 2000, Hiram College; JD 2003, Northeastern University of Law; MLS 2010, Indiana University

PAUL E. SALAMANCA, Wyatt, Tarrant & Combs Professor of Law. AB 1983, Dartmouth College; JD 1989, Boston College

ROBERT G. SCHWEMM, William L. Matthews, Jr. Professor of Law. BA 1967, Amherst College; JD 1970, Harvard University

BEAU STEENKEN, Instructional Services Librarian. BA University of Texas at Austin; MA, Texas State University-San Marcos; JD, University of Texas School of Law; MS, University of Texas School of Information; LLM, University of Nottingham, United Kingdom

RICHARD H. UNDERWOOD, William L. Matthews, Jr. Professor of Law. BA 1969, JD 1976, The Ohio State University

RYAN VALENTIN, Head of Public Services. JD 2004, University of Oregon; MLIS 2007, Florida State University

HAROLD R. WEINBERG, Everett H. Metcalf, Jr. Professor of Law. AB 1966, JD 1969, Case Western Reserve University; LLM 1975, University of Illinois

SARAH N. WELLING, Ashland-Spears Distinguished Research Professor of Law. BA 1974, University of Wisconsin; JD 1978, University of Kentucky

RICHARD A. WESTIN, Professor of Law. BA 1967, MBA 1968, Columbia University; JD 1972, University of Pennsylvania

ANDREW K. WOODS, Assistant Professor of Law. BA 2002, Brown University; JD 2007, Harvard University; PhD 2012, University of Cambridge

ADJUNCT FACULTY

GLEN S. BAGBY, Adjunct Professor of Law. BA 1966, Transylvania University; JD 1969, University of Kentucky. Firm: Dinsmore & Shohl

FRANK T. BECKER, Adjunct Professor of Law. JD 1979, University of Kentucky. Equine and Commercial Law and Litigation Practitioner
DON P. CETRULO, Adjunct Professor of Law. BA 1971, Morehead State University; JD 1974, University of Kentucky. Firm: Knox & Cetrulo

JENNIFER COFFMAN, Adjunct Professor of Law. BA 1969, JD 1978, University of Kentucky. Retired Chief Judge of the Eastern District of Kentucky

REBECCA DILORETO, Adjunct Professor of Law. BA 1981, Amherst College; JD 1985, University of Kentucky. Children's Law Center

ANDREW DORISIO, Adjunct Professor of Law. BS 1980, West Virginia University; JD 1996, University of Kentucky. Firm: King & Schickli

JANET GRAHAM, Adjunct Professor of Law. BS 1987, Virginia Tech University; JD 1991, University of Kentucky College of Law. Commissioner of Law, Lexington-Fayette Urban County Government

KAREN GREENWELL, Adjunct Professor of Law. BA 1976, JD 1985, University of Kentucky. Firm: Wyatt, Tarrant & Combs

PIERCE W. HAMBLIN, Adjunct Professor of Law. BBA 1973, JD 1977, University of Kentucky. Firm: Landrum & Shouse

JAMES G. HARRALSON, Adjunct Professor of Law. JD 1979, University of Kentucky. Retired Associate General Counsel for AT&T Mobility

JOHN HAYS, Adjunct Professor of Law. BA 1985, Princeton University; JD 1988, University of Kentucky. Firm: Jackson Kelly

G. EDWARD HENRY II, Adjunct Professor of Law. BA 1976, JD 1979, University of Kentucky. Firm: Henry, Watz, Raine & Marino

GAYLE W. HERNDON, Adjunct Professor of Law. JD 1982, University of Kentucky. Retired Tax Counsel for Tax Policy and Planning at the General Electric Company

PAULA HOLBROOK, Adjunct Professor of Law. BS 1990, JD 1993, University of Kentucky. UK HealthCare

GUION JOHNSTONE, Adjunct Professor of Law. BA 2005, Transylvania University; MSW 2011, JD 2011, University of Louisville. Director of Maxwell Street Legal Clinic

EMILY JONES, Adjunct Professor of Law. JD 2011, University of Kentucky. Immigration Attorney at Kentucky Refugee Ministries

RAYMOND M. LARSON, Adjunct Professor of Law. JD 1970, University of Kentucky. Fayette County Commonwealth Attorney

JOHN T. MCGARVEY, Adjunct Professor of Law. BA 1970, JD 1973, University of Kentucky. Firm: Morgan & Pottinger

GEORGE MILLER, Adjunct Professor of Law. BA 1975, AM 1978, Brown University; Ph.D 1981, Brown University; JD 1984, University of Kentucky. Firm: Wyatt, Tarrant & Combs

MARGARET PISACANO, Adjunct Professor of Law. BSN 1980, Vanderbilt; JD 1983, University of Kentucky. Associate General Counsel and Director of Risk Management at University of Kentucky's Chandler Medical Center

DAMON PRESTON, Adjunct Professor of Law. BA 1991, Transylvania University; JD 1994, Harvard. Deputy Public Advocate
STEVEN ROUSE, Adjunct Professor of Law. AB 1999, University of Illinois; JD 2006, Northwestern University

THALETIA ROUTH, Adjunct Professor of Law. JD 2000, University of Kentucky. Associate General Counsel for University of Kentucky

THOMAS E. RUTLEDGE, Adjunct Professor of Law. BA 1985, St. Louis University; JD 1990, University of Kentucky. Firm: Stoll Keenon Ogden

LINDA SMITH, Adjunct Professor of Law. BA 1997, Transylvania University; JD 1994, Northern Kentucky Salmon P. Chase College of Law

LARRY SYKES, Adjunct Professor of Law. BA 1975, Vanderbilt University; JD 1983, University of Kentucky. Firm: Stoll Keenon Ogden

WILLIAM THRO, Adjunct Professor of Law. BA 1997, Transylvania University; JD 1990, University of Virginia School of Law

M. LEE TURPIN, Adjunct Professor of Law. BA 1997, Transylvania University; JD 1992, University of Kentucky College of Law. First Assistant County Attorney

ANDREA WELKER, Adjunct Professor of Law. BA 1997, Transylvania University; JD 2009, University of Kentucky College of Law

CHARLES WISDOM, Adjunct Professor of Law. JD 1985, University of Louisville. Chief, Appellate Section, US Attorney’s Office

JEFFREY YOST, Adjunct Professor of Law. JD 1972, West Virginia University; LL.M. 1979 Georgetown University. Firm: Jackson Kelly PLLC