Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:10(4), October, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed : Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available : www.ijmer.in

CONTEMPORARY THREATS TO THE UNITED STATES: INTERNATIONAL RIVALRIES, CYBERSECURITY VULNERABILITIES, AND GLOBAL CHALLENGES

Ms. Kakani Sisira Bhumika
MA – International Relations &Political Science, Freelance Scholar, Central University of Kerala

Abstract

The United States is dealing with a messy and ever-changing security situation that's tough to handle using old methods. This paper takes a shot at looking at three of the biggest problems: the return of intense competition with China and Russia, the growing danger of cyberattacks, and the ongoing issue of global threats like terrorism and organized crime. People usually study these things separately, but I think they're all linked. Because they're interconnected, it's harder to deal with them. That means we need strategies that work together, focusing on both stopping threats overseas and making us stronger here at home. This analysis uses official reports, think-tank studies, and some academic work. It's not meant to be a complete picture, but just a student's contribution to the conversation about how the U.S. can juggle its many priorities in the future.

Introduction

Since the Cold War ended, what the U.S. considers important for security has changed several times. In the 1990s, it was about peacekeeping and globalization. The 2000s were all about fighting terrorism after 9/11. More recently, U.S. strategy papers—especially the ones from 2017 and 2022—say that competition with big powers is the main challenge. They call out China and Russia as rivals who want to change things. But other problems haven't gone away. Cyberattacks threaten our systems every day, and global networks—from fentanyl dealers to terrorist organizations—still make us unsafe at home and around the world.

So, the U.S. isn't just facing one big danger, but a bunch of pressures all coming together. Russia's attack on Ukraine in 2022 wasn't just a war; it also involved cyberattacks on Ukraine and Europe, plus fake news campaigns aimed at people in the West. Also, China's competition with the U.S. in high-tech areas directly affects both our economy and our military strength. Meanwhile, smaller groups often take advantage of the weaknesses that major powers' rivalries and new technologies create.

The big question this paper asks is: How do these areas—strategic competition, cyber warfare, and global threats—connect, and what does that mean for U.S. security? I think that U.S. policy often treats these things as separate, when they're actually related. To show this, I'll look at relevant studies and then analyze each threat. The paper ends with some thoughts on what this means for policy, with a focus on being strong at home and deterring threats abroad.

Literature Review

The academic world has lots to say about U.S. national security. You can generally break it down into three main topics, even though they definitely overlap:

1. Big Power Showdown

Some experts, like John Mearsheimer, think the world is going back to the old days of countries competing for power. He sees China's rise as a problem, and expects the U.S. and China to butt heads more and more. Graham Allison chimes in with his idea about the "Thucydides Trap," which warns that history shows rising powers and established powers often end up fighting. While these ideas are important, they also have critics. Guys like Joseph Nye say we don't have to see the U.S. and China as just military rivals. Nye talks about "smart power," using both strength and diplomacy, and thinks they could work together on things like climate change. Personally, I like Nye's take, but I think he might be a bit too hopeful, considering how China's acting in the South China Sea.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:10(4), October, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed : Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available : www.ijmer.in

2. Digital Security

Here, there's a split between people who don't think cyber stuff is a big deal and those who think it's completely changing the game. Thomas Rid famously said "cyber war isn't going to happen," arguing that most cyberattacks are just spying or messing around, not real warfare. That doesn't sound so convincing now, especially after the Colonial Pipeline hack that freaked everyone out by messing with gas supplies. Others, like Richard Clarke and Robert Knake, say cyberspace is the new "fifth battleground," like land, sea, air, and space. This debate isn't over, but the reality is that countries and groups keep pushing the limits of what they can do online.

3. Worldwide Dangers

Because of globalization, it's getting harder to tell the difference between problems at home and problems abroad. Experts like Tamara Makarenko talk about a "crime-terror connection," showing how criminals and terrorists often share resources and help each other out. More recent work, like Katz's, looks at how terrorists get their money through things like drug dealing. Another area focuses on climate change as something that makes other problems worse (as Busby puts it). They point out how environmental issues can cause more trouble in places like the Sahel or the Middle East. Compared to the big power and cyber debates, this area sometimes feels less important to the big picture of U.S. strategy, but it's still important on the ground, especially for law enforcement and security.

In general, these different areas of study give us some good ideas, but they tend to stay separate. People who study China or Russia often don't think much about cyber issues, while cyber experts sometimes forget how countries competing affects things. Also, terrorism and organized crime are often treated as separate from big power competition. This paper tries to bring these things together (in a general way), to show how they connect instead of treating them as separate.

Analysis

- Who's Challenging the US: China and Russia

When we think about who's competing with the US on a global scale, China is definitely the biggest worry for the long haul. Their money-making strategies – like "Made in China 2025" and the "Belt and Road Initiative" – aren't just about buying and selling; they're about shaping the world the way they want it. What's especially concerning is how China mixes its financial goals with its military ambitions, particularly in fields like computer intelligence, computer chips, and super-fast computing. Their military upgrades, especially with ships and rockets, show that they aren't just aiming to be a powerful economy – they want to change the rules in the Asian-Pacific region. The Taiwan Strait is like a tense situation; the constant military drills there suggest China is seeing how far they can push things. Also, China's efforts to reshape international groups to support "cyber control" and different ways of developing show that they're not just trying to show off military might – they're trying to change the way people think about running countries.

Russia, on the other hand, is a different kind of problem. They're not as strong financially, but they've found ways to make a big impact, mainly through clever and unexpected moves. The Ukraine invasion in 2022 showed that Russia is ready to use strong-arm tactics, backed up by its nuclear weapons. But their power isn't just military – they also use computer attacks, misleading information, and control over energy supplies. For example, cutting off gas to Europe has become a common way for them to get what they want politically. Outside of Europe, the use of private military groups like the Wagner Group demonstrates Russia's creative, if harsh, approach to influencing things – projecting its strength in places where the US and NATO can't easily react.

China and Russia aren't exactly best friends, but their teamwork on diplomatic issues – especially in fighting back against Western punishments – is interesting. For the US, this creates a tough situation: resources are stretched, and some worry that focusing too much on "joined-up defense" could overextend things. There's also the question of whether focusing so much on global rivalries leaves the US weaker at home.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:10(4), October, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed : Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available : www.ijmer.in

- Cyber Warfare: The Expanding Battleground

Computer security is one of those areas where the rules are still being made up, which makes it both exciting and scary. Countries, particularly China and Russia, have made computer attacks a common strategy. Stealing secrets and messing with elections are just the beginning. Events like the Colonial Pipeline attack in 2021, even though it was done by criminals, showed how weak our important systems really are. Finding out who's responsible is a huge problem – proving who did it is rarely simple, which makes preventing future attacks feel almost impossible.

Ransomware (where hackers hold data for money) and criminal groups add another layer of difficulty. Hospitals, schools, and local governments have been targeted again and again, often with attacks coming from places where law enforcement is weak or where the government lets it happen. The amount of money lost and the disruption caused is massive, sometimes billions of dollars each year. It really makes you wonder if governments and private companies are working together fast enough on computer security.

And then there's misleading information, which is arguably harder to fight than a computer attack on a pipeline. The Russian interference in the 2016 US election is a good example – social media becomes a weapon that's cheap, effective, and hard to trace. These campaigns don't just bother people; they can really damage trust in democratic institutions. Efforts by groups like CISA show some attempt to make our cyber defenses better, but weak points in computer hardware and software remain. Internationally, agreeing on rules for the internet seems super slow, probably because the major powers just don't agree.

- Transnational Threats and Global Insecurity

Threats from groups and problems that aren't specific to one country remind us that insecurity isn't just about China or Russia. Terrorism, even though it doesn't control as much land, has spread out more. ISIS, for example, now relies heavily on recruiting people online, and Al-Qaeda related groups are still active in Africa. Attacks by individuals inspired online make stopping these threats even harder.

Organized crime, especially international groups, adds another level of worry. Drug dealing, arms dealing, and human trafficking show how these groups can act like mini-countries, and the US opioid crisis is a strong reminder that these networks have real, direct effects at home.

Climate change, while not a direct actor, makes everything more complicated. Droughts and lack of resources cause people to move, create instability, and make regions like the Sahel good places for crime and terrorist recruitment. It's not often thought of as a "security threat" in the usual sense, but its indirect effects are huge. Ignoring it in security planning seems more and more dangerous.

Conclusion

To wrap things up, the dangers facing the U.S. today aren't simple or from just one place. They come from a mix of big countries competing, online fights, and problems that cross borders. Often, those in charge deal with these things separately, but they're really connected, making things trickier. For instance, China's money goals are tied to stealing secrets online, and Russia uses sneaky, mixed tactics to push its power. Meanwhile, groups that work across borders – whether they're criminals or terrorists – use technology and world problems to their advantage.

The big challenge for the U.S. seems to be finding the right mix. If we focus too much on military strength, we might forget to make our own country strong. But if we only focus on getting ready at home, our rivals might freely challenge our influence in the world. A better way is to do both: build strong friendships with other countries while also putting money into important things at home like roads and bridges, online security, and making sure people feel united.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:10(4), October, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed : Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available : www.ijmer.in

Ultimately, winning isn't just about fighting off threats. It's also about keeping our democratic system and values strong, because those are what make the U.S. a leader in the world. Without them, any advantage we have won't last long.

Bibliography

1. Council on Foreign Relations (CFR). "The U.S. Immigration Debate." Accessed September 30, 2025. https://www.cfr.org/backgrounder/us-immigration-debate-0?hl=en-IN
2. Marshall Center. "Russia and China's Intelligence and Information Operations Nexus." Accessed September 30, 2025. https://www.marshallcenter.org/en/publications/clock-tower-security-series/strategic-competition-seminar-series/russia-and-chinas-intelligence-and-information-operations-nexus?hl=en-IN
3. National Security Agency (NSA). “Strategic Environment.” Accessed September 30, 2025. https://www.nsa.gov/About/Strategic-Environment/
4. Office of the Director of National Intelligence (ODNI). *Annual Threat Assessment of the U.S. Intelligence Community*. Washington, DC: ODNI, 2025. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf
5. Sisson, Melanie W. "The China-Russia Relationship and Threats to Vital U.S. Interests." Brookings Institution, June 28, 2023. https://www.brookings.edu/articles/the-china-russia-relationship-and-threats-to-vital-us-interests/
6. The White House. *National Security Strategy, October 2022*. Washington, DC: The White House, 2022. https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf