

# Problematic Researchers and Supply Chain Risk

Problematic researchers pose alarming new risks to U.S. national security, supply chains, and critical infrastructure. Wittingly and unwittingly, these researchers expose potent technology breakthroughs to malign foreign actors through normal research activities and cultures.

Open, collegial research cultures increase national security vulnerabilities in three ways:

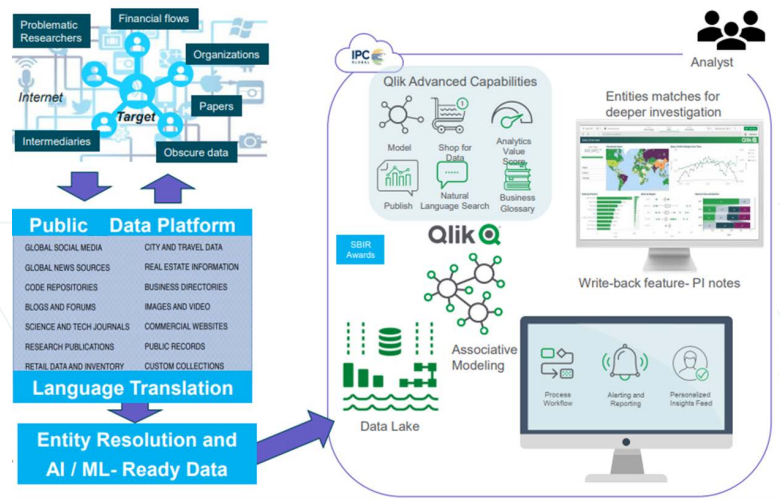
- Creating undetected gaps in military and civilian technology development ecosystems
- Expanding the attack surface exposed to cybersecurity and supply chain threats
- Obscuring and blending financial flows between legitimate and malign funding sources

Only advanced analytics - combining historic, real-time, and public data - can counter these risks. This investigative capability must include in-memory data associations, all-source market sensing, and process automation to support diverse economic and security analysis teams.

Qlik uniquely overcomes these challenges by ingesting more data sources than anyone else, automating analytical processes, and maturing the workforce's use of analytics. This drives trusted decisions, automated discovery, workforce data literacy, and governed information sharing with approved agency stakeholders.

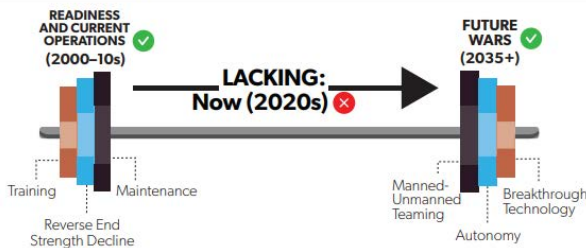
IPC Global has validated a Qlik solution that meets these requirements using public data from Vertical Knowledge. It connects diverse data sources, enables entity discovery, automates manual forensic activities, surfaces related and unrelated data values, performs high-speed calculations, and provides clean data visualizations in operational context.

Successful actors exploiting problematic researchers can disrupt global markets and technology ecosystems permanently. Intellectual property (IP) theft costs far less than research and development (R&D) at scale, giving a sustainable economic advantage to these malign actors. For example, in 2020, Dr. Charles Lieber, Chair of Harvard’s Department of Chemistry and Chemical Biology and a recipient of U.S. Government funding from civilian and defense agencies seeking big nanotechnology breakthroughs, was arrested and charged with fraud and falsehood for failing to disclose his contracts with the Wuhan University of Technology, a well-established foreign talent recruitment program.



MACKENZIE EAGLEN WITH HALLIE COYNE

Figure 2. Barbell Military Investment Strategy Was Unbalanced: We Are in the “Lacking 2020s”



Source: Author.

Modernization of U.S. military platforms now costs over \$400 billion per year, more than 30% of U.S. defense spending. Military programs now face a significant R&D gap. Researchers like Lieber dot this landscape, exposing strategic IP from military platforms, intelligence systems, and supply chains across hundreds of acquisition programs and thousands of contractors to thousands of actors from foreign talent programs.

IPC Global’s solution is built for the scale of the challenge. It definitively responds to the strategic calculus behind the threat. It connects a broad data ecosystem to modernize the investigative process by leveraging existing agency technologies and adding Qlik and partner technologies where relevant. This solution has improved analytical workflows by 50% or more.

A rare bipartisan consensus now recognizes the scale of this facet of great power competition today. A new U.S. industrial policy was signed on June 9, 2021 to protect and strengthen U.S. supply chains and sensitive technology sectors from talent recruitment programs. Senator Chuck Schumer enumerated the strategic threat in stark terms: “[A]uthoritarian governments...believe that squabbling democracies like ours can’t come together and invest in national priorities the way a top-down, centralized and authoritarian government can.”

Though the digital scale of the problem is new, Carl von Clausewitz forecast the solution to such ancient tactics of duplicity in 1832: “But in war more than in any other subject we must begin by looking at the nature of the whole; for here more than elsewhere the part and the whole must always be thought of together.”

Qlik’s solution leverages the power of the cloud for information sharing yet operates under strict enterprise governance for privacy and security. It can be demonstrated and deployed rapidly for new customers to create powerful network effects between agencies already working holistically to use all available data for analytics to take measured actions to mitigate this growing risk.

### About Qlik

Qlik’s vision is a data-literate world, one where everyone can use data to improve decision-making and solve their most challenging problems. Only Qlik offers end-to-end, real-time data integration and analytics solutions that help organizations access and transform all their data into value. Qlik helps companies lead with data to see more deeply into customer behavior, reinvent business processes, discover new revenue streams, and balance risk and reward. Qlik does business in more than 100 countries and serves over 50,000 customers around the world. [qlik.com](https://www.qlik.com)