

QICR

Quadrennial Intelligence
Community Review

FINAL REPORT

April 2009



Office of the Director of National Intelligence

SECRET//REL TO USA, FVEY

SECRET//REL TO USA, FVEY



FINAL REPORT

April 2009



(U) FOREWORD

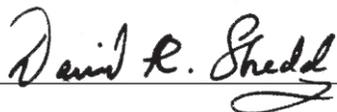
(U) If one does not consider the long-range future, one will never cease to be surprised. The Director of National Intelligence (DNI) has an annualized planning/programming process to guide short-term (1-5 years) perspectives. The *National Intelligence Strategy (NIS)* and *Vision 2015* provide mid-term (5-10 years) perspectives. The Quadrennial Intelligence Community Review (QICR) provides an essential long-term piece, looking out between 10 and 20 years. This longer term view complements shorter term assessments, challenges basic assumptions, exposes the potential risks of extrapolating tomorrow's needs from today's conditions, and examines missions and capabilities in light of alternative futures.

(U) This report describes the results of the 10-month QICR. Building on the National Intelligence Council's *Global Trends 2025: A Transformed World*, experts from across the Intelligence Community (IC), other U.S. departments and agencies, academia, think tanks, and industry assessed the implications of the year 2025 for the IC.

(U) QICR 2009 developed alternative future scenarios based on *Global Trends 2025* to explore concepts and capabilities the IC may need to fulfill critical missions in support of U.S. national security. It does not purport that any one future will materialize, but rather outlines a range of plausible futures so that the IC can best posture itself to meet the range of challenges it may face.

(S//REL) This Final Report summarizes six concepts for how the IC may need to operate by 2025. Of particular note, QICR 2009 identifies three concepts that are critical to the success of the IC across a wide range of future scenarios ("safe bets") and suggests that these concepts merit attention in the IC's longer term planning efforts, including the *NIS*, Intelligence Planning Guidance, and other guidance documents. The first concept is the development of a sensing and learning environment capable of handling massive amounts of information (*Sentient Enterprise*). The second is the adoption of a more dynamic and tailored customer-services model (*Segmented Customers, Differentiated Services*). The third is the adoption of an expeditionary mindset that can project operational capability and enhanced analytic connectivity in both physical and virtual venues (*Responsive Presence*).

(U) We hope this report will stimulate spirited debate and rigorous thinking as to how the IC can best posture and prepare for a range of future environments.



April 21, 2009

David R. Shedd
Deputy Director of National Intelligence
Policy, Plans & Requirements



(U) EXECUTIVE SUMMARY

(U) Introduction. The Quadrennial Intelligence Community Review (QICR) 2009 used scenario-based analysis to help the Intelligence Community (IC) consider how to best minimize strategic surprise and manage institutional risk to meet challenges that may emerge by 2025.

(C//REL) Drawing on the National Intelligence Council's *Global Trends 2025: A World Transformed*, QICR made three key assumptions about the future landscape for intelligence. First, other actors will increase in power and relevance relative to the United States. Second, the information environment will radically transform in scope, complexity, and intensity, with intelligence targets operating seamlessly and simultaneously between the physical and virtual worlds. Third, customers and the IC workforce will be "digital natives" with different operating models and expectations for how to perform and leverage the business of intelligence.

(U) Concepts for Intelligence in 2025. In this landscape, certain organizing principles for performing intelligence functions—"concepts" in this report—could help turn future challenges into opportunities. QICR identified three concepts ("safe bets") that appear critical to the success of the IC across a wide range of possible futures and therefore merit consideration in today's long-term planning activities.

- (C//REL) *Sentient Enterprise* is an IC that creates a sensing and learning environment for humans and intelligent machines to analyze "exabytes" of data in near-real time to generate and test hypotheses, autonomously process and evaluate insights to cue collection, and self-update/self-correct.
- (C//REL) *Segmented Customers, Differentiated Services* envisions an IC postured to provide more customized tools, products, and services to an expanding set of customers with different styles and end uses.
- (C//REL) In *Responsive Presence*, the IC has an expeditionary intelligence capacity to deploy small teams to hostile (physical or virtual) environments with minimal infrastructure, while readily drawing on more diverse and instantly collaborative analytic expertise to guide operations and directly leverage the insights gained.

(U) "Strategic hedges" are concepts deemed highly relevant in some possible futures but less relevant in others, which the IC may need to develop as circumstances warrant.

- (C//REL) *Technology Acquisition by All Means* envisions the IC aggressively employing a mix of overt means, clandestine penetration, and counterintelligence tactics to address severe U.S. technological erosion vis-à-vis near-peer competitors and global corporations.
- (C//REL) In *Human Terrain in the Virtual World*, the IC confronts environments dominated by non-state actors, requiring unconventional human collection methods with more flexible sets of analytic partners to track highly empowered, cyber-immersed individuals and groups.
- (C//REL) *Money Mastery* describes an operating concept that requires the IC to compensate for the possible loss of access to reliable financial and economic data (at the global, national, and sector levels) by penetrating corporations, foreign finance ministries, central banks, and market participants to create an "economic operating picture."

(S//REL) Conclusion. Four broader implications arise from the QICR 2009. First, the IC will have to manage highly fluid relationships to deal with the dynamism of a more competitive national security environment. Second, it will need to manage a singular operational architecture to deal with the new ways that a greater volume of information will flow. Third, the IC will need to maintain strong information and identity assurance to address the likely erosion in its technological advantage and the new dynamics of the digital medium. Fourth, the IC will need to change the role of the intelligence officer to deal with a dynamic external environment and adapt to new customer needs. To posture the IC to deal with these implications, QICR suggests the value of further study by appropriate IC elements in the areas of policy, regulation, and law; organization and structure; workforce management; and information and identity assurance.

(U) TABLE OF CONTENTS --- ---

(U) INTRODUCTION	1
(U) Methodology.....	1
(U) Key Assumptions	2
(U) CONCEPTS FOR INTELLIGENCE IN 2025.....	5
(U) Safe Bet: Sentient Enterprise	6
(U) Safe Bet: Segmented Customers, Differentiated Services	8
(U) Safe Bet: Responsive Presence.....	10
(U) Strategic Hedge: Technology Acquisition by All Means	12
(U) Strategic Hedge: Human Terrain in the Virtual World	14
(U) Strategic Hedge: Money Mastery.....	16
(U) CONCLUSION	19



(U) INTRODUCTION

(U) Every 4 years, the Intelligence Community (IC) assesses the most challenging issues it could face beyond the standard planning cycle. This process is known as the Quadrennial Intelligence Community Review (QICR).

(U) QICR 2009 was a scenario-based strategic planning activity that looked out to the year 2025 and considered alternative future environments (i.e., “scenarios”), missions the IC might be called on to perform, and the concepts and some illustrative capabilities that would be needed to fulfill those missions. This Final Report summarizes the key findings and recommends next steps to help position the IC to address the challenges of the future.

(U) Methodology

(U) The QICR 2009 applied best practices of scenario planning used in both industry and government. Using as a starting point *Global Trends 2025: A Transformed World*, produced by the National Intelligence Council (NIC), QICR developed four scenarios that were designed to be divergent, plausible, challenging, and relevant to the IC. These scenarios are not predictive, but illustrate the range of possible challenges we might confront. QICR organized the scenarios along two key dimensions of uncertainty—the relative importance of the nation-state and the extent of global cooperation—and then incorporated additional relevant features of possible future environments gleaned

from seven recognized geo-strategic scenario sets developed by public, private, U.S., and foreign sources. (See the *QICR Scenarios Report*, January 2009, for a full discussion of the scenarios.)

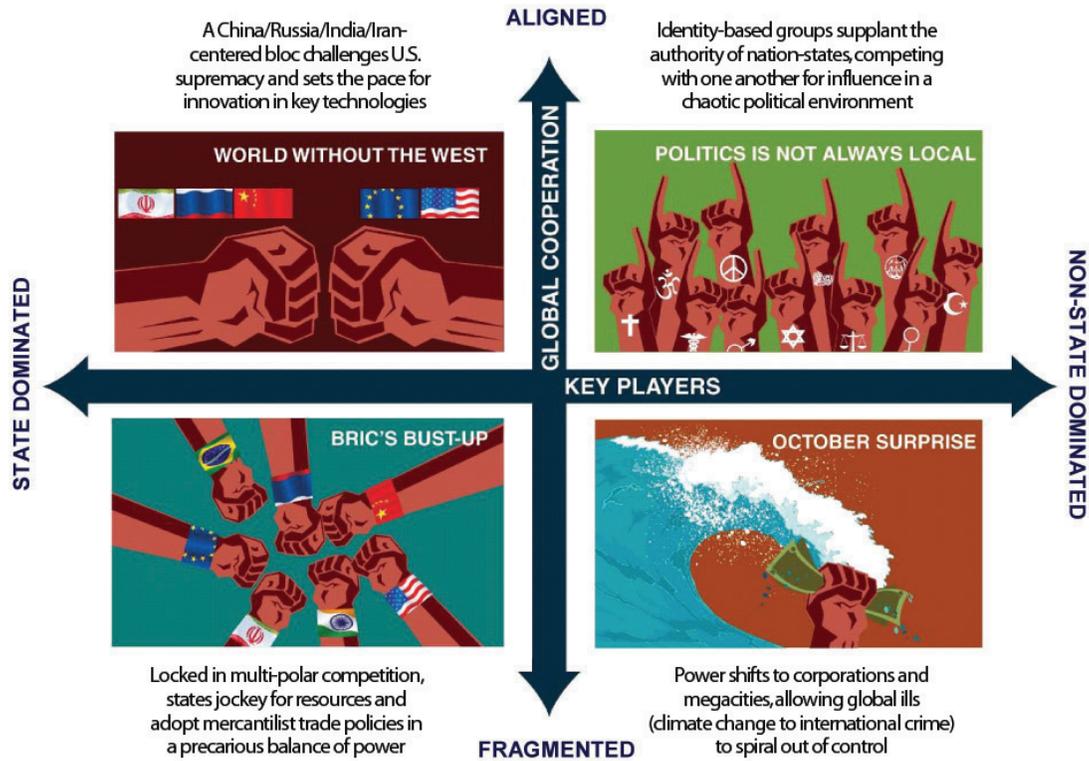
(U) The scenarios served as the basis for analysis of missions the IC might be asked to perform in support of national objectives and the concepts and capabilities the IC would need to perform these missions. (The four scenarios are summarized in the figure on page 2.) Each scenario implied a core set of missions for the IC that was not exhaustive but highlighted the key demands customers would likely place on the IC in 2025 beyond the array of established intelligence activities:

- (C//REL) *World Without the West*: Although a coalition of four well-armed competitor states calls for continued robust military analysis, understanding energy, natural resources, and technological innovation emerges as a critical mission for the IC.
- (C//REL) *BRICs* Bust-Up*: As the United States struggles to maintain its world standing amidst competing and insular blocs, the IC is predominantly focused on economics and commercial science and technology (S&T) missions.
- (C//REL) *Politics Is Not Always Local*: With non-state affinity groups driving international politics, the IC is focused on transnational threats, particularly crime and cyber attack.

* (U) The acronym BRIC refers to Brazil, Russia, India, and China, or more generally, the big developing economies.



(U) QICR Scenarios



- (C//REL) *October Surprise*: Amidst the rise of mega-corporations as the purveyors of traditional state functions, the IC focuses on uncovering economic, financial, and corporate ground truth, as well as on providing early warning on outbreaks of infectious disease and natural disasters.

(U) QICR developed concepts to illustrate how today's operating model will have to change for the intelligence enterprise to remain effective. QICR identified two sets of concepts. Concepts that were critical to the success of the IC across all the scenarios were labeled "safe bets," indicating that we should begin planning for their eventual adoption. Concepts that were critical to only one or two scenarios were deemed "strategic hedges," implying that we should experiment with

them and consider long-lead development of essential elements, while monitoring ongoing events to assess whether more aggressive action is appropriate.

(U) The QICR process also delineated sample capabilities to clarify the intent and impact of these concepts for activities, people, technology, etc. These capabilities are not meant to be either definitive or exhaustive, but rather serve as a starting point for further analysis.

(U) Key Assumptions

(C//REL) Based on the NIC's *Global Trends 2025* study, the QICR identified three key assumptions that set the context for the future posture of the IC. First, the United States will remain among the most prominent

forces in world politics, but the **relative ascent of other state and non-state actors** across the full range of power dimensions—military, economic, technological, and social—will place new and different demands on the IC.

- (C//REL) The proliferation, differentiation, and sophistication of actors in global politics will make it far more difficult to access targets (whether in the physical or virtual world), maintain a consistent and continuous presence, and influence populations.
- (S//REL) With more tenuous U.S. technological leadership in key sectors such as biotechnology, nanotechnology, and computing, the IC may have less unilateral advantage in critical intelligence capabilities (e.g., penetrating encrypted information networks).
- (S//REL) The IC will increasingly rely on information and communication technology that is at least partly of foreign origin, rendering critical IC functions more vulnerable to attack or manipulation in increasingly hard-to-detect ways.

(C//REL) The second key assumption about the world in 2025 is the **transformation in the information (and thus cyber) environment**, specifically in the volume, velocity, and variability with which information flows between and among individuals, groups, and states. This new environment will be enabled by two parallel and reinforcing phenomena: the incorporation of sensors and processors into many more items (from weaponry to foodstuffs) and almost universal access to inexpensive networked computing and communications technologies. As such, there will be an exponential increase in the amount of data of all types potentially available to the IC, its U.S. Government customers, hostile governments, and adversary non-state actors.

Information will also move at ever increasing speeds, and it will exist in greater ranges of formats that change more frequently.

- (C//REL) Most intelligence targets will increasingly operate simultaneously in the physical and virtual worlds, requiring the IC to adopt a seamless approach between the two domains as well.
- (C//REL) Balancing intelligence with the protection of privacy and civil liberties will be even more challenging in 2025. The IC will need socially, constitutionally, and politically acceptable ways to handle exponentially more information no matter what future comes to pass. In many cases, meeting the challenge will come down to more effective data management. Automated analysis of “anonymized” data could detect threats much earlier without infringing upon privacy. Role-based access could help mitigate the risk of abuse.

(C//REL) The third key assumption about the operating environment of 2025 is that **IC customers and partners will be “digital natives”** and will have a significantly different set of expectations of the IC. They will tend to behave in two fundamentally different ways, both of which contravene current orthodoxy.

- (U) Having grown up with the likes of *Wikipedia*, *Facebook*, *Flickr*, and *Google Earth*, customers will be accustomed to building their own context, understanding, and in many cases, technical details.
- (U) Customers will be much less reliant on official intermediaries and much more comfortable reaching out directly to networks of experts and data (whether or not they are inside the IC).



(U) CONCEPTS FOR INTELLIGENCE IN 2025

(U) To cope with the challenging missions emerging from the four scenarios summarized in the figure on page 2, QICR developed six concepts (see figure below) that point to a need for further exploration and potential investment. Some of these concepts will be critical across the full spectrum of possible futures and thus are termed **“safe bets”** because they merit the most urgent attention for further development and investment. Other concepts will be highly relevant in a narrower range of future operating environments, although aspects of the concept may have wider application. These concepts are termed **“strategic hedges,”** and merit further exploration for investment in the event that future developments point toward their increasing importance. Together, these concepts and their associated sample key capabilities highlight how the management, organization, and practice of intelligence must evolve to cope with the range of alternative futures the IC may confront. The IC will need to develop innovative approaches, potentially including some adaptation of the legal and/or policy framework under which the IC operates.





(U) Safe Bet: Sentient Enterprise

(U) In 2025, electronic data will have increased exponentially as massive amounts of stored data have accumulated and access to mobile communications and networked sensors have become ubiquitous. The volume, velocity, and variability of data will pose enormous search and knowledge-management challenges, driving the IC toward non-linear processing and autonomous organization of critical information. Virtual interactions will be integral to daily communications for millions of benign purposes, but hostile actors will also use this medium as a means to build ideological and financial support and for planning and execution of operations. In addition, signals of threats may be few, weak, or conflicting because of the ability to shelter activity from domains that require a signature.

(C//REL) The concept of *Sentient Enterprise* postures the IC for this circumstance, creating a sensing and learning environment capable of identifying and responding to voluminous, simultaneous, and continuous inputs. The *Sentient Enterprise* will track and manage thousands of exabytes of data every day (1 exabyte is the equivalent of 100,000 times the Library of Congress, which holds 19 million books), enabling iterative assessments in real time, not days or weeks. The data it manages will be universally discoverable, accessible, and usable by humans and machines equally. Indeed, the human-machine interface will allow the individual to interact directly with a unified information architecture. The enterprise will be able to continuously and autonomously process, evaluate, and act on new data without regard to structure or format. The enterprise will log expert users' interactions with the data, while gleaning new insights from more generalist users. By so doing, the entire enterprise will create, share, and advance corporate knowledge in a rich and seamless interplay where machines and humans learn together.

(U//FOUO) The *Sentient Enterprise* will have the additional benefit of freeing intelligence professionals from mundane tasks so that they can focus on activities reliant on human judgment. Analysts will be able to allocate much more of their time to the front and back ends of the intelligence cycle, focusing much more energy on scoping problems with customers, driving collection, and helping customers understand the implications of different courses of action. More seasoned officers will be able to more ably mentor novices, collaborate with other experts, and influence decision-makers.

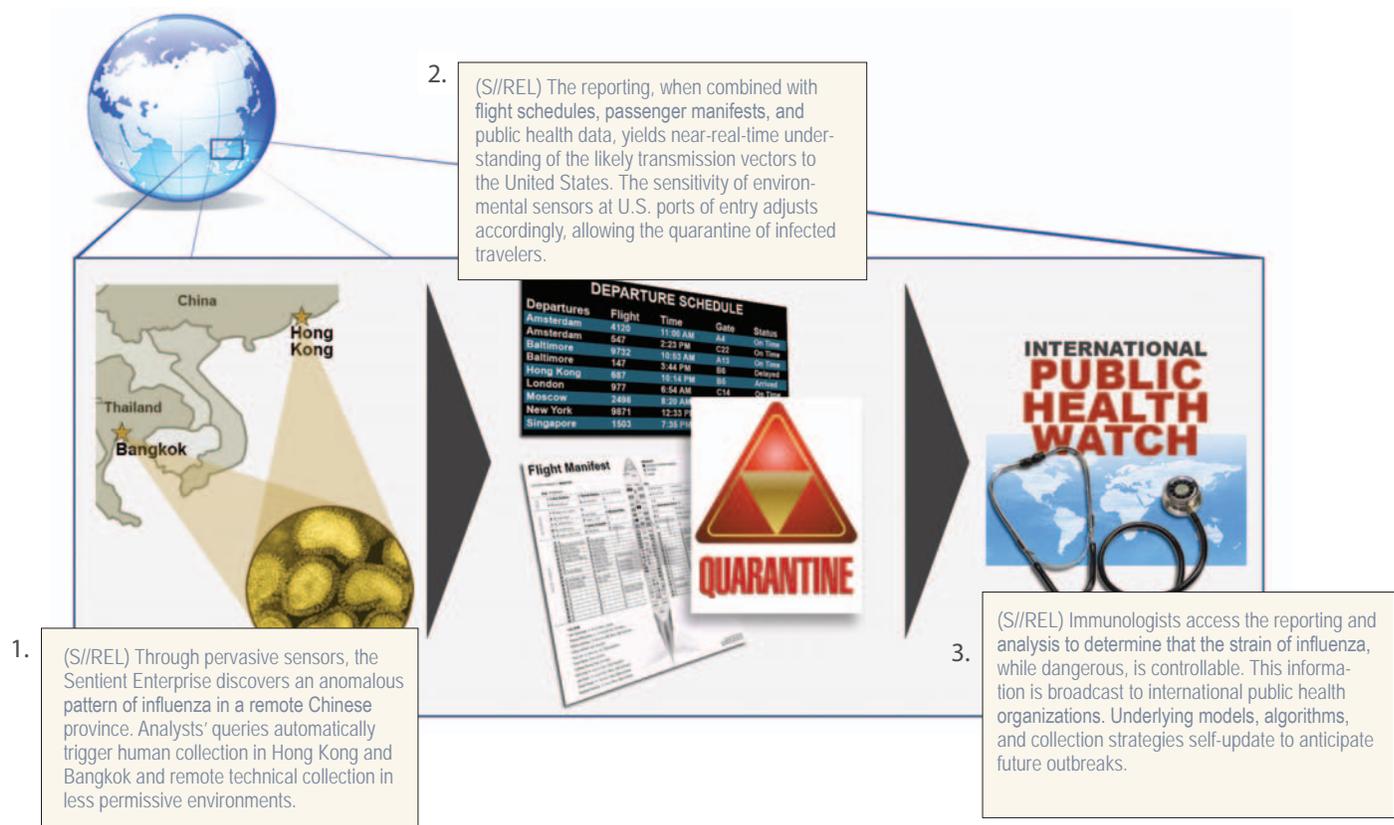
(U) Sample Key Capabilities

- **(C//REL) Automation.** The IC would emplace sensors and monitor applications that run autonomous collection of the most relevant data, trigger pattern recognition sequences, and process raw feeds. This would require supercomputer-like capabilities at every "computational point-of-presence," from computer terminal to digital handheld device. Automation (e.g., in language translation, gisting, relational analysis, and trend assessment) would allow verification and validation of the accuracy of information.
- **(U) Artificial Intelligence (AI).** Application of advanced AI techniques would make it possible to continuously improve understanding of complex threat environments, discern the relative importance of data, and adapt quickly to changes indicated by sensor data and automated analysis (thus providing indication and warning). This would allow the experts to focus on translating critical information to decision-makers in an effective and time-efficient manner.

- **(S//REL) Self-Learning.** The institutional knowledge of the *Sentient Enterprise* would increase the user’s ability to recall events and significant facts to build relational awareness. Simultaneously, the human-machine interface would enable the user to continuously refine the “algorithms” that translate human judgments into machine language so that the system actively learns.
- **(U) Human Interface.** The *Sentient Enterprise* would employ dashboards and similar interfaces to provide continuous, real-time visualization of the operational environment. Interfaces would include interactive touch-screen mapping of a large variety of data types that enables zoom and pan capabilities to scan the physical, virtual, and social environments.
- **(U) Collaborative Features.** The *Sentient Enterprise* would employ social-networking tools and virtual models of the real world to monitor the threat environment, enable collaboration, and test alternative hypotheses. This would include social-networking tools that allow outside experts to be tapped quickly so they could make contributions in a crisis and provide input into the analytic process.
- **(S//REL) Protection.** The continuously updated, multilayered, and changing boundaries of *Sentient Enterprise* would be selectively permeable, requiring innovative system or data-specific protection capabilities for flow of data into and out of the data stream.

Illustrative Example

(U) Sentient Enterprise





(U) Safe Bet:
Segmented Customers, Differentiated Services

(U) The expectations of digitally native users and a much more diverse set of partners will drive a different conceptualization of the customer. First, the IC will engage its customers with greater responsiveness, employing highly iterative customer segmentation, requirements, and satisfaction analyses to understand their working styles and decision-making needs. Second, the IC will focus its efforts on more tailored services (e.g., visualization techniques and tabletop role-play exercises), vice products, to meet the full spectrum of customer needs. Third, the IC will provide data and analyses anywhere (in U.S.-based offices or in the field), in more dynamic ways (from interactive streams available via wireless devices to immersive, three-dimensional presentations), and at multiple classifications.

(U) The concept of *Segmented Customers, Differentiated Services* synthesizes these conclusions with a construct of three categories of customers. These categories are not dissimilar to today, but their needs will be met with different capabilities. At one end of the spectrum, “do-it-yourself” customers will want data and analytic tools from the IC so they can answer their own questions. In the middle of the spectrum are users of analytic products who will expect to see—and work with—the un-

derlying data and models, frequently in collaboration with the IC. At the other end of the customer spectrum are users who will turn to analysts for tailored analysis and products that they can apply without further refinement or context.

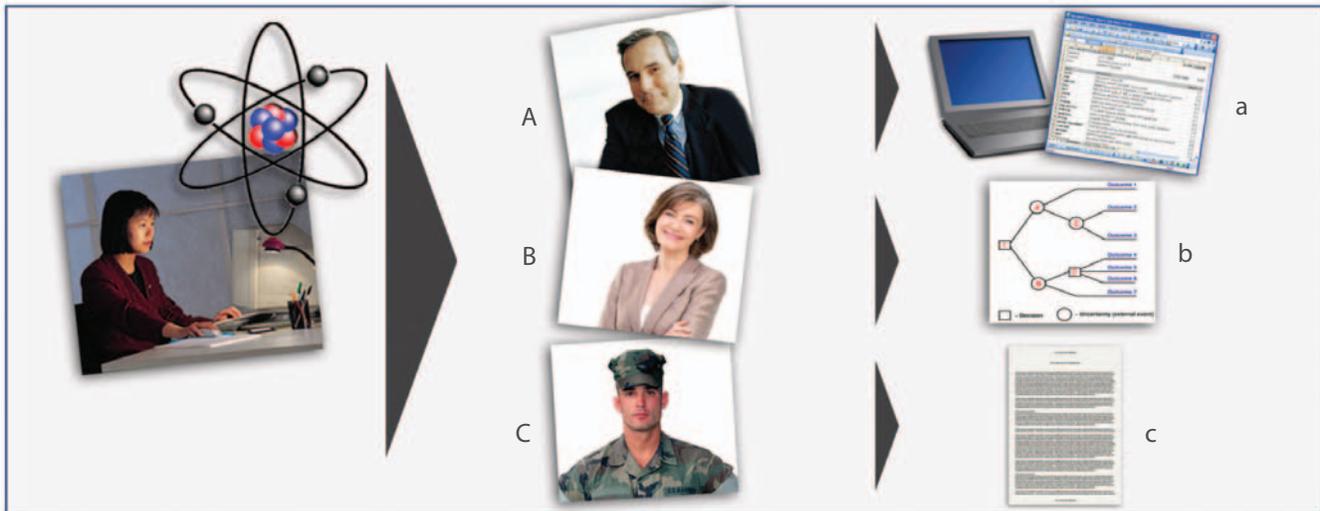
(U) Sample Key Capabilities

- **(C//REL) Interactive Visualization.** The IC would deploy dashboards, datastreams, and other interfaces that allow customers to continuously monitor the operational environment, rather than rely on static judgments.
- **(C//REL) Interactive Tools.** Interactive decision-support tools would allow customers to conduct their own sensitivity analyses, test hypotheses, and discover new insights from underlying data, either with or without an intelligence officer assisting.
- **(C//REL) Customization.** Customer interfaces would enable users to enter specific requirements, update them dynamically, and build tailored products in various forms and for various media.

Illustrative Example

(U) Segmented Customers, Differentiated Services

1. (C//REL) With global tensions on the rise as a Middle Eastern state says it will “go nuclear” absent United Nations (UN) concessions, a senior weapons of mass destruction (WMD) intelligence analyst maintains robust and differentiated support to three key customers.



2. (C//REL) The National Security Council director for counterproliferation (A) looks to the analyst to ensure the latest operational data goes directly to his secure laptop (a). The State Department’s top arms-control negotiator (B) calls on the analyst to help her prepare for an upcoming session by walking her through an immersive simulation using the latest intelligence (b). The commander of a multi-national task force in the Indian Ocean (C) asks the analyst for a tailored, releaseable intelligence product (c).



(U) Safe Bet: Responsive Presence

(C//REL) In 2025, the United States will face much greater difficulty penetrating key states that suddenly emerge as areas of national security interest. It may have neither an extensive forward military presence nor much of a physical diplomatic and intelligence presence, depriving it of an understanding of the socio-cultural environment. Adding to the challenge, despite the transformation in the information environment, nation-states in some scenarios may try to cord off their information infrastructures into national intranets. In such a world, the IC will need a way to rapidly deploy suites of intelligence capability (collection, analysis, security, communications, etc.) over the horizon to theaters of political-military competition where U.S. Government presence and infrastructure are minimal or have been withdrawn. In addition, the IC will need to be prepared to deploy its resources in cyberspace to meet quickly emerging challenges.

(C//REL) *Responsive Presence* addresses this challenge by applying the expeditionary model developed in the military context, bringing the capability of an overseas station to bear when and where necessary. It builds on today's deployable organizational models and rests on several principles: development of small tactical teams capable of rapid deployment and long, autonomous operation in a variety of environments; a small logistical and communications footprint that is largely carry-in/carry-out; and a robust, self-sufficient communica-

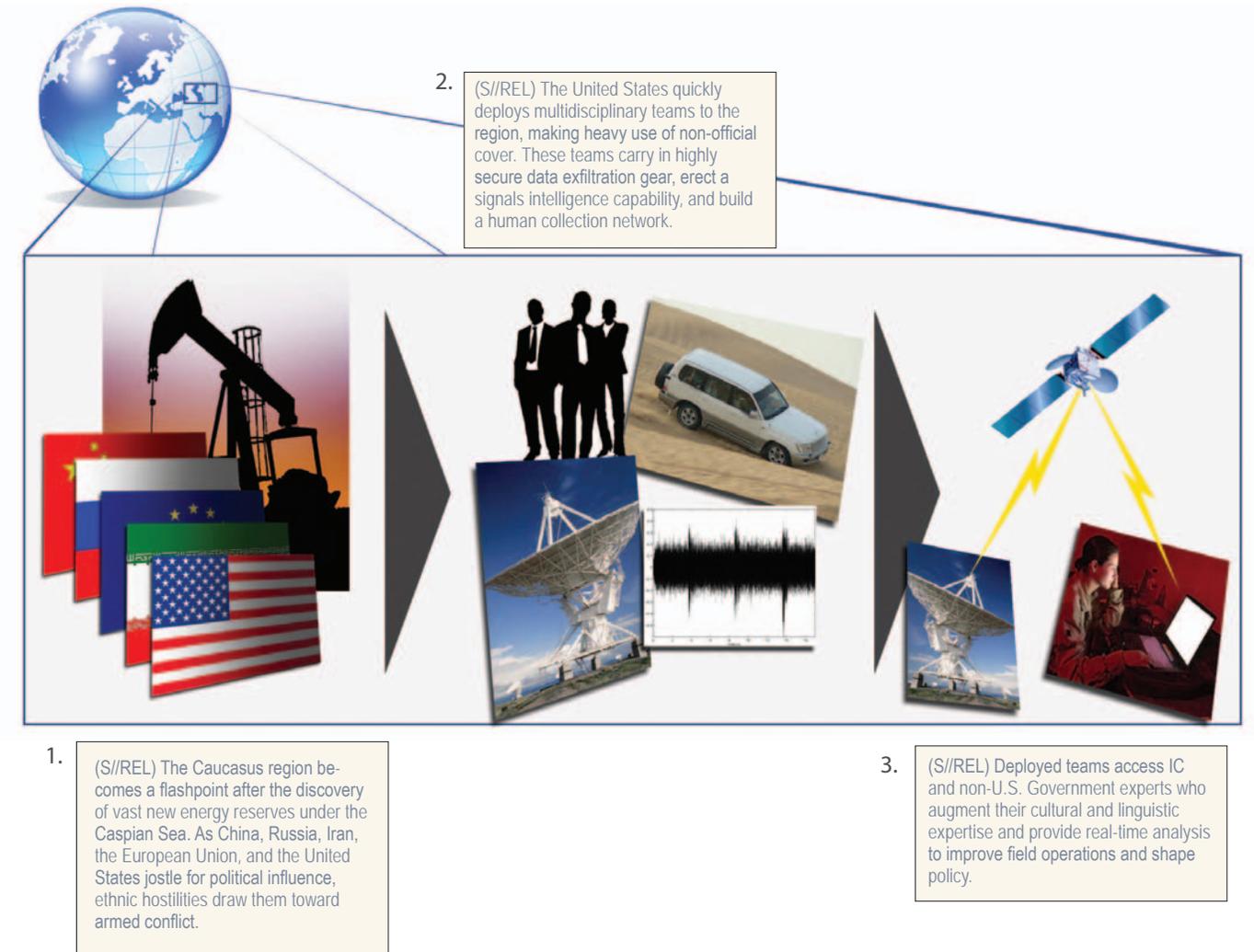
tions capability. Similarly, the intelligence enterprise will need a cyber architecture that can rapidly move into IT network "clouds" undetected and maintain that presence with few additional resources.

(U) Sample Key Capabilities

- **(S//REL) Data Exfiltration and Covert Communications.** Exfiltrating intelligence from non-permissive environments will be crucial. A critical enabler would be covert communications with a negligible forward footprint. U.S. intelligence officers and sensitive sources will need to move data in an unattributable and undetected way, sometimes from within commercial entities possessing great technical prowess and robust cyber and electronic security protective procedures. Although the likely advent of transnational, high-bandwidth wireless communications services will offer an environment with "lots to hide behind," it will also contain many highly competent, and potentially antagonistic, actors.
- **(S//REL) Expanded Reachback.** Deployed units would have ready reachback to a heterogeneous set of expert analysts from IC elements, other U.S. Government departments, academia, and non-governmental organizations. They would have trusted and secure means to communicate with these partners that would enable real-time exchange while protecting the most sensitive operational details.

Illustrative Example

(U) Responsive Presence





(U) Strategic Hedge: Technology Acquisition by All Means

(C//REL) QICR identified two scenarios in 2025 in which the United States' technological and innovative edge slips—despite our countervailing efforts—and shifts to denied areas. Under one scenario, a bloc of states actively seeking to undermine U.S. geostrategic leadership could deny access to key emerging technologies. Another possibility is that the technological capacity of foreign multinational corporations could outstrip that of U.S. corporations. The IC would be challenged to understand technological innovation outside its traditional competencies (e.g., weapons systems) and in domains where it traditionally has focused less effort (e.g., commercial research and development (R&D)). Because technological advancement tends to be exponential rather than linear, either development could put the United States at a growing—and potentially permanent—disadvantage in crucial areas such as energy, nanotechnology, medicine, and information technology.

(C//REL) To offset risk in these particular futures, the IC would need to deploy a set of entrepreneurial tactics to maintain a technological advantage. This concept rests on a multi-pronged, systematic effort to gather open source and proprietary information through overt means, clandestine penetration (through physical and cyber means), and counterintelligence.

(U) Sample Key Capabilities

- **(S//REL) S&T Analysis.** The IC would monitor scientific and trade journals, patent filings, and other “gray material” datastreams, enabled by technologies associated with *Sentient Enterprise*, to discover latent patterns that precede technological innovation. Thus, the IC would be better able to manage the problem of “tens of analysts” sifting through “thousands of pages.”
- **(S//REL) “Thousands of Conversations.”** The IC would need the ability to access proprietary sources of information in permissive environments such as foreign universities, industry trade shows, and government conferences. This could include cooperating U.S. students, professors, and researchers reporting bits of non-public information that by themselves are not sensitive, but in aggregate could help the IC make inferences about breakthrough technological innovations. The key challenge would be working closely with the academic and scientific communities (which would include non-U.S. persons), gaining trust, and monitoring potential “threats” while continuing to advance U.S. scientific progress.
- **(S//REL) Direct Penetration.** In denied or more restrictive environments such as state-supported R&D centers, the IC would continue to apply human intelligence (HUMINT) tradecraft and employ HUMINT-enabled close access collection. This would include recruitment of sources and assets, and provision of appropriate technical means to acquire and exfiltrate sensitive information.

- **(S//REL) Cyber Operations.** The IC would sustain close-access collection, frequently by second and third parties, to non-public and/or covert centers of innovation by implanting applications (i.e., bots) that run automated tasks and sensors in software and hardware used by foreign researchers and manufacturers, and by conducting computer-network exploitation of foreign R&D intranets. In select instances, this could also involve development of long-term sources.

- **(C//REL) S&T Counterintelligence.** Counterintelligence in both the public and private sectors would not rely solely upon defensive measures, but would also undertake proactive measures to detect, identify, and degrade or neutralize foreign efforts to illegally acquire U.S. technology in areas where we retain a leadership position. Counterintelligence would actively seek out and engage foreign entities involved in illicit intelligence collection operations using offensive methods and become as effective in the cyber sphere as in the physical sphere.

Illustrative Example

(U) Technology Acquisition by All Means





(U) Strategic Hedge: Human Terrain in the Virtual World

(C//REL) In 2025, non-state identity and affinity groups operating seamlessly across physical and virtual worlds could be the key players in global politics. Some of these groups could pose a grave challenge to U.S. political legitimacy and physical security. In virtual worlds, individuals could tailor multiple personas for different settings, and both individuals and groups could have many overlapping or non-obvious relationships. Therefore, understanding the different roles an individual or group might play in multiple contexts would represent the central challenge around which the IC would be oriented.

(S//REL) In this circumstance, the IC would increasingly need to employ a virtual presence to complement its physical presence. That presence would include maintaining a forward position inside unconventional partner and target entities by routinely embedding officers not only in foreign intelligence services, as it does today, but also in cooperative non-state groups. The IC would also routinely employ private citizens as proxies for sensitive analytic and collection tasks. Academics, business people, and others would form an IC-led standing dialogue, participating in collaborative analytic teams when and as their expertise warranted.

(U) Sample Key Capabilities

- **(S//REL) The Virtual IC.** The IC would require collection approaches and counterintelligence capabilities such as online techniques for human collection. Developing and protecting online cover personas and authenticating the identity of online sources and data would continue to be critical elements of HUMINT and counterintelligence tradecraft.
- **(S//REL) Bridging Domains.** An automated cross-cueing of collection platforms, including distributed sensors, would maintain a seamless approach to monitoring and understanding individuals and groups as they move between and operate across the physical and virtual worlds.
- **(S//REL) Identity Assurance.** As it builds a web of complex and shifting partnerships, the IC would need fail-safe means to authenticate its partners' identities, conduct counterintelligence, and control access to its most sensitive intelligence, which will be more challenging in 2025 than today due to the proliferation of key technologies.
- **(S//REL) Counterintelligence.** The IC would develop increasingly effective methods for detecting, deterring, and exploiting hidden foreign manipulation of IC activities, and recognizing the trusted insiders who are threats. Offensively, the counterintelligence target of choice would shift to persons

who have access to identity or affinity groups assessed as a threat to U.S. national security. These targets would be more likely to be located in commercial or private establishments and might have no discernible affiliation with a nation-state actor.

- **(C//REL) Trusted, Deployable, Diverse Workforce.** Organizationally, the IC would need to more aggressively recruit and maintain a more diverse workforce capable of penetrating and analyzing affinity-based groups. In many cases, this would require hiring from such groups—and dealing creatively with the counterintelligence challenges presented by the multiple loyalties that such recruits would be likely to have.

Illustrative Example

(U) Human Terrain in the Virtual World

1. (S//REL) Rapid but unevenly shared advances in human enhancement have spawned transnational interest groups focused on medical ethics. Some question limiting human enhancement to the wealthy few; others reject it altogether. These communities use virtual environments to form and proselytize, although some form physical communes to live “unenhanced” lifestyles.

3. (S//REL) IC and law enforcement agencies conduct human intelligence in both physical and virtual environments. Automated software tools help concatenate commercial, sensor, and open-source data to verify targets using multiple online personas. Academic experts help IC analysts better understand how online interest groups self-organize, grow, and splinter into extremist elements.



2. (S//REL) Although most groups focus on peaceful political change, U.S. law enforcement and the IC become aware of an extremist subcurrent, which they are concerned could lead to “medical terrorism.”



(U) Strategic Hedge: Money Mastery

(C//REL) If corporations, megacities, and foreign governments were to limit access to data critical to the provision of global public goods such as macro-economic stability, U.S. policymakers could come to rely on the IC to assist in efforts to collect and analyze this closely held financial and economic information and create an “economic operating picture” similar to the “common operating picture” the military strives for today. Basic elements of today’s financial intelligence (e.g., international datasets maintained by the International Monetary Fund and others, government reports, and industry analyses) would be unavailable, unreliable, or misleading.

(C//REL) In this case, the IC would need a concept of *Money Mastery* to penetrate corporations, markets, foreign central banks, and foreign finance ministries and organizations so that it could gather and analyze proprietary data. The IC also would need to track critical commodities markets in much greater detail as well as the full range of illicit financial markets and economies. This concept would far exceed today’s approach to financial and economic intelligence in scale and scope and would require increasingly sophisticated targeting expertise, even more aggressive HUMINT collection, and processing tools.

(U) Sample Key Capabilities

- **(S//REL) “White/Grey/Black” Literature Exploitation.** Overtly, the IC would monitor open markets in stocks, commodities, and currencies. To acquire non-public but unprotected data such as proprietary business information, it would use two-way information sharing with trusted and cooperative corporations and foreign governments. Clandestinely, the IC would use human and technical means, including sophisticated tracking software, to access closely held market, financial, and business data, be it inside corporations, foreign governments, or other institutions.
- **(C//REL) Geoeconomic Analysis.** Intelligence professionals would monitor the stability of the global economic system (not just single nation-state economies) for early warning of disruptions and would help policymakers understand the implications of different policy interventions.
- **(S//REL) Verify and Validate.** The IC would assume an even greater validation function to discern the truth in official economic data issued by nation-states and multilateral organizations. To do this, the IC would employ a standing collaborative network of economic experts—drawn from many sectors of the economy, business, and governmental bodies, foreign and domestic—while mitigating the potential insider threat.

Illustrative Example

(U) Money Mastery

1. (S//REL) A handful of international city-states and mega-corporations have bypassed multilateral forums to establish their own carbon cap-and-trade regime. Most trading of carbon credits occurs through private channels that are opaque to financial regulators (U.S. or otherwise).

3. (S//REL) Covertly, IC agencies form front corporations to participate directly in the market and employ spyware that detects speculative trading—a leading indicator of systemic risk in this market. The findings help the United States build international support for stronger oversight.



2. (S//REL) Concerned that this burgeoning market could trigger a global financial crisis, a network of IC and non-IC government agencies overtly partners with U.S. energy and carbon-abatement corporations to acquire non-public information about the carbon-credit market.



(U) CONCLUSION

(U) QICR 2009's charge was to build on and distill the implications of the NIC's *Global Trends 2025* so that IC leadership could begin to manage the risks associated with plausible alternative future environments challenging to the nation and the IC. This Final Report highlights six concepts (three "safe bets" and three "strategic hedges") and identifies a number of illustrative capabilities that would enable these concepts. IC elements are strongly encouraged to deepen and broaden the discussion of safe bets and strategic hedges begun here, and to begin to consider whether and how stronger foundations for these concepts might be laid into the next several planning and programming cycles.

(C//REL) Collectively, these findings imply four broader implications for how to posture the IC to deal with the range of uncertainty in 2025. First, the IC will have to **manage highly fluid relationships** to deal with the dynamism of a more competitive security environment and the fluidity among partners, sources, and targets. This will require the IC to accept more risk despite increasingly complex counterintelligence and security challenges.

- **(C//REL) Varying Patterns.** The IC will need to maintain both enduring partnerships grounded in deep trust and shared interests as well as marriages of convenience that are ephemeral and ad hoc. Relationships with foreign partners, in particular, will have to be much more variegated and extend to unorthodox allies, be they states or non-state actors.
- **(C//REL) Range of Partners.** The IC will need to more aggressively leverage outside expertise (foreign and domestic, governmental and non-governmental) across all facets of the intelligence

enterprise (from collection to security to technology development). Reliance on outside expertise will require a commensurate level of vigilance in the form of effective counterintelligence to ensure the integrity of information and systems are protected. Equally important, the IC will have to recruit, train, educate, mentor, and retain a sufficiently sized cadre of intelligence professionals capable of sustaining a rigorous dialogue with external experts. Finally, the IC will need to continue developing products and services for state, local, and tribal governments as well as the private sector, recognizing that these customers have specialized information needs and generally do not have access to classified information systems.

- **(C//REL) Changing Roles, Unknown Attributes.** The IC will need ways to deal with partners whose roles vis-à-vis U.S. security interests change rapidly. Partners or sources in one dimension may very well be intelligence targets in another. Additionally, the IC will have to deal with actors who more actively conceal their physical locations, nationalities, true identities, and true purposes. The IC's operating and management model (to include tradecraft) will have to work across jurisdictions and domains to deal with these challenges, which probably will mandate a more robust collection and analytic posture inside the United States.

(S//REL) Recommendation: Appropriate elements of the IC should conduct a policy, regulatory, and legal review to ensure the IC can meet the challenges of highly fluid relationships in ways that respect the desire of the American people for privacy and civil liberty.



(S//REL) Second, the IC will need to **manage a singular operational architecture** that allows for the discovery and tracking of targets across domains, be they physical or virtual, foreign or domestic, in order to deal with the new ways that a greater volume of information will flow. Continued access to, and effective use of, space will likely serve as a critical enabler to provide important collection and communication capability to work across this divide, although it may be challenged in scenarios where states or corporations compete for primacy in space. Achieving such an architecture will be more difficult if and when U.S. rivals attempt to militarize space and/or endeavor to increase significantly the risk to U.S. space-based intelligence assets. At the same time, the IC will need to maintain visibility into “off-the-grid” activity that has no digital signature or a very ambiguous physical signature but that can still have disproportionately large effects.

- **(C//REL) Dynamic Interaction.** The IC will need an architecture capable of adapting quickly as threats and issues emerge and readily cueing collection and operations, often across the physical and virtual domains.
- **(C//REL) Few, Conflicting, or Weak Signals.** The IC will need to synthesize data from multiple, often novel, sources to identify threats or opportunities. In particular, the IC will need to anticipate, detect, understand, and place into context digital signals that have few, if any, physical manifestations.

(S//REL) Recommendation: Appropriate elements of the IC should assess the organization and structure of the intelligence enterprise to ensure it will support the kind of operational architecture necessary to deal with the transformed information environment of 2025.

(U) Third, the IC will need to **change the role of the intelligence officer** to deal with a dynamic external environment and adapt to new customer needs. The IC will need officers trained in multiple fields, from technology to methodology to all-source analysis, with many filling multiple roles at the same time. The workforce model will need profound reassessment in at least two dimensions:

- **(C//REL) Building Well-Rounded Experts.** IC personnel will still need specialized training, including in languages, but they will require deeper understanding of context to perform their jobs. Initiatives like joint duty will need to be greatly expanded and complemented with an array of developmental, educational, and training activities.
- **(C//REL) Cross-Training.** The IC will need to prepare intelligence professionals for careers in which the distinction between analyst and collector is increasingly irrelevant, particularly in virtual worlds. At the same time, the IC will need to build teams to bring a range of skills to bear on complex problems, because some degree of individual specialization will persist.

(U) Recommendation: Appropriate elements of the IC should review how to adapt the workforce management model to promote flexibility, responsiveness, collaboration, and appropriate incentives and rewards.

(S//REL) Fourth, the IC will need to **maintain strong information and identity assurance** to address the likely erosion in our technological advantage and the new dynamics of the digital medium, which will introduce new risks to our IT infrastructure and new methods of denial, deception, and misdirection.

- **(S//REL) Declining IT Security.** The IC will have to operate in an environment where computing infrastructure is more difficult to secure, advanced encryption is far more pervasive, and our cryptologic advantages may persist only in niches where we have focused resources to achieve breakthroughs. Indeed, the IC may not be able to provide comprehensive security for its entire IT infrastructure and may have to use such offsetting strategies as “hide in plain sight.”
- **(S//REL) Digital Deception.** The IC will need to operate in an increasingly virtual operational environment where denial, deception, disinformation, and hostile collection will intensify the risks posed to collection systems and analytical methodologies. Recognizing the difference between clandestine adversaries and non-threatening interlocutors will require new sets of knowledge, skills, and abilities from our HUMINT, security, and counterintelligence cadres.
- **(S//REL) Identity Assurance.** The IC will need robust ways to discover, manage, and protect identities as many more people use multiple online personas and leverage increasingly sophisticated anonymizing techniques. It will need approaches to mitigate this challenge by taking advantage of linked identities and entities providing a web of potentially identifying information to cue social-network analysis.

(C//REL) Recommendation: Appropriate elements of the IC should assess the information and identity assurance capabilities of the IC to ensure it will be able to meet the digital challenges of 2025.

(U) In conclusion, QICR 2009 highlights the urgency to begin developing new approaches to prepare for an uncertain future. Elements of the National Intelligence Program, foreign intelligence services, state, local, and tribal governments, and industry are encouraged to consider these insights in conducting their own long-term planning efforts. The rigor with which QICR 2009 developed these ideas to mitigate strategic and institutional risk must now be translated into meaningful agenda items for the IC and its partners to carry forward.



(U) For additional reading:

- (U) National Intelligence Council, *Global Trends 2025: A Transformed World*, December 2008, available at http://www.dni.gov/nic/NIC_2025_project.html.
- (U) Office of the Director of National Intelligence, *Quadrennial Intelligence Community Review Scenarios: Alternative Futures the IC Could Face*, January 2009.

SECRET//REL TO USA, FVEY

SECRET//REL TO USA, FVEY



Office of the Director of National Intelligence