April | 2017

# US-DiGIA: Mapping the USG Discoverable Information Terrain

## Sources of national security and foreign policy information with a focus on gray zone identification and response activities

Prepared for

Strategic Multi-Layer Assessment

Gray Zone Conflicts, Challenges, and Opportunities: A Multi-Agency Deep Dive Assessment

Project Team: Belinda Bragg, Ph.D.; Sabrina Pagano, Ph.D.; John A. Stevenson, Ph.D.

POC: Belinda Bragg, bbragg@nsiteam.com

Deeper Analyses
Clarifying Insights
Better Decisions

www.NSIteam.com

**Citation:** Bragg, B. (2017). *US-DiGIA Directory: Mapping the USG Discoverable Information Terrain.* Arlington, VA: Strategic Multi-layer Assessment (SMA).

# Table of Contents

# Introduction

The United States faces a complex and dynamic security environment. States are no longer the only critical actors in the international arena; rather, a diverse range of non-state entities also has the potential to affect US interests and security—for good or bad. Economic influence, information control and propaganda, political influence, and social discontent can be and are being utilized by state and non-state actors alike to achieve their goals, in many cases bypassing the need for direct military action. In response, the US military is challenged to accomplish more, across a greater variety of domains, while facing a constrained budget environment.

Recent SMA projects demonstrate a clear awareness that success in this current international environment requires broadening how we think about the military's role in securing US interests. USPACOM and USEUCOM have requested projects designed to examine "future political, security, societal, and economic trends to identify where US interests are in cooperation or conflict" with China and Russia respectively. USCENTCOM has sought "population and regional expertise in support of ongoing operation in the Iraq/Syria region." This current USSOCOM gray zone project builds on Gen. Votel's observation that "if the USG is to respond effectively to the threats and opportunities presented in the increasingly gray security environment, it requires much more thought and nuanced understanding of the space between peace and war."

All of these requests share an underlying theme: for the US military to do its job in the evolving security environment, it needs to move beyond its expertise in traditional military domains and reliance on kinetic solutions. Economic, human, cognitive, and other domains are critical factors in the US government's ability to respond to and shape the current security environment. There are two central implications of this: first, many of the most intractable security problems the US faces require a whole of government approach. Second, in a complex and evolving international environment characterized by new and often ambiguous threats, information itself is a critical asset.

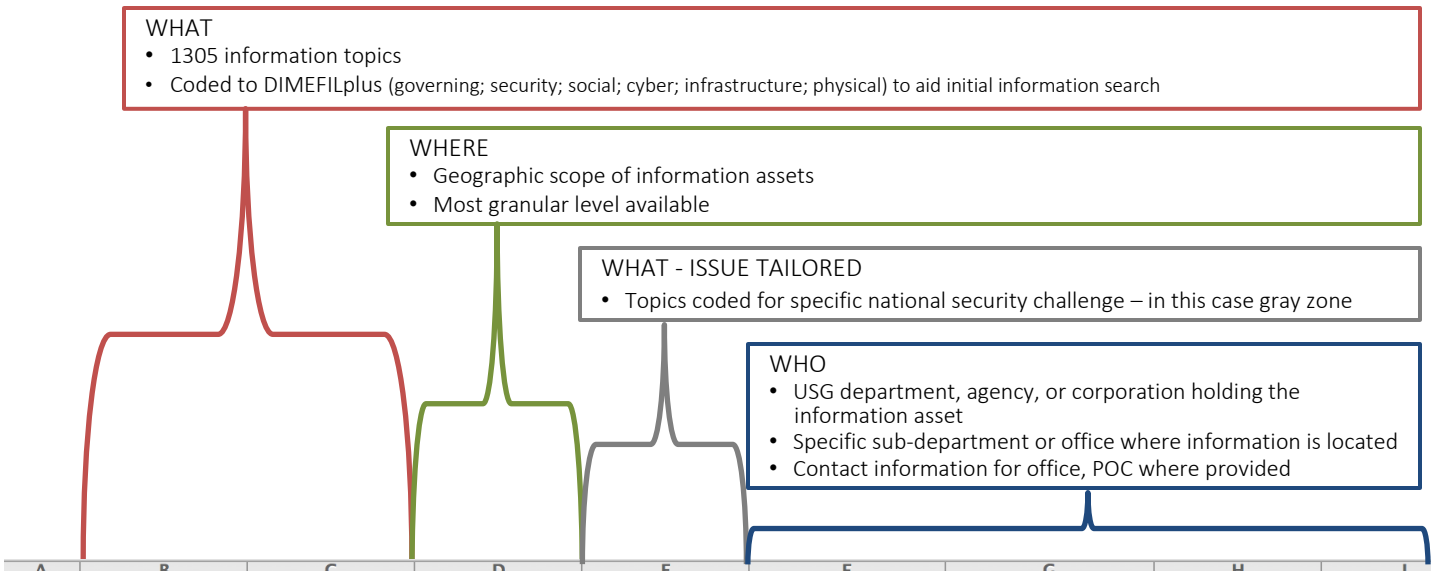
The United States Government collects, analyzes, and reports on an impressive range of topics, many of which are relevant to this broader understanding of national security. If USSOCOM and others were able to leverage these existing extant sources of information, data, and expertise (i.e. *information assets*), the cost and time savings from avoiding duplication of effort would be potentially immense.

This can only happen, however, if people are able to identify, locate, and access these information assets easily. Currently there is no catalogue of the information housed within and across the entirety of USG organizations. This creates a significant barrier to information sharing and the development of the interagency collaboration required for implementation of whole of government solutions to security challenges.

## US-DiGIA Directory: Mapping the Information Terrain

In an effort to reduce this barrier, the NSI team "mapped" the USG information terrain, cataloguing all discoverable (unclassified, published, and referenced or held online) information assets relevant to national security and foreign policy held across the non-DoD and non-ODNI USG organizations. This effort resulted in the Directory of Discoverable US Government Information Assets (US-DiGIA),

which provides a tool that enables users to search for and locate open source USG information assets and possible points of contact for interagency collaboration. The structure of the US-DiGIA is shown in Figure 1 below.




| A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|
| Entry ID | Information Topic | DIMEFILplus | Geographic Region | Gray Zone Element | Organization | Office | Website | Contact |
| 1543 | arms_exports | economic | international | arms_exports | department_of_state | directorate_of_defense_tra | http://www.pmddtc. | |
| 1547 | arms_exports_embar | governing | international | arms_exports | department_of_state | directorate_of_defense_tra | http://www.pmddtc. | |
| 1546 | arms_exports_policie | governing | international | arms_exports | department_of_state | directorate_of_defense_tra | http://www.pmddtc. | |
| 1593 | arms_small_and_light | security | international | arms_exports | department_of_state | office_of_weapons_remova | http://www.state.go | |
| 1322 | arms_small_and_light | law_enforcement | central_america | arms_trafficking | department_of_state | western_hemisphere_affai | http://www.state.go | Giovanni Snidl |
| 1323 | arms_small_and_light | law_enforcement | north_america | arms_trafficking | department_of_state | western_hemisphere_affai | http://www.state.go | Giovanni Snidl |
| 1596 | arms_small_and_light | law_enforcement | international | arms_trafficking | department_of_state | office_of_weapons_remova | http://www.state.go | |
| 1512 | arms_trade_treaty | diplomatic | international | arms_exports | department_of_state | office_of_conventional_arr | http://www.state.go | |
| 1545 | arms_trafficking_inte | diplomatic | international | arms_trafficking | department_of_state | directorate_of_defense_tra | http://www.pmddtc. | |
| 1443 | arms_transfers | economic | international | trade_arms | department_of_state | arms_control_verification_ | http://www.state.go | |
| 1787 | asian_development_b | financial | asia_pacific | banking_internationa | department_of_the_treas | international_financ | | |
| 0943 | asset_forfeitures | law_enforcement | united_states | assets | department_of_justice | criminal_division_as | | |
| 0946 | asset_forfeitures | law_enforcement | united_states | assets | department_of_justice | us_marshals_office | | |
| 1049 | asset_forfeitures | law_enforcement | international | assets | department_of_justice | criminal_division_of | | |
| 1821 | asset_forfeitures | law_enforcement | united_states | assets | department_of_the_treas | office_of_terrorism_ | | |
| 1826 | asset_forfeitures | law_enforcement | united_states | assets | department_of_the_treas | office_of_terrorism_ | | |

The US-DiGIA Directory, with user guide, is available from the POC upon request

Figure 1: US-DiGIA Directory Format

The US-DiGIA captures three critical aspects of discoverable USG information:

1. *What* information, relevant to national security writ large the USG collects and holds
2. *Who,* specifically within the USG, collects and holds that information
3. *Where* geographically the information assets are focused

The US- DiGIA Methodology Report provides a full discussion of the coding rules used for constructing the US-DiGIA, and is available on the SMA publications website.

Though the NSI team's effort was bounded by the discoverability of the information assets reported by each organization, the resulting directory nonetheless uncovered over 1,900 relevant individual information assets in various forms (e.g. reports, datasets, SME knowledge) across 21 USG executive branch organizations. A brief discussion of the scope and limitations of the directory can be found in Appendix A.

We cast a wide net when determining relevance to security and foreign policy, including in the US-DiGIA information related to:

- US and foreign state military capacity
  - E.g.: armed forces data; weapons data
- Security and diplomatic agreements and relations
  - E.g.: arms trade treaties; security cooperation; arms control
- Physical environment
  - E.g.: geospatial data; infrastructure
- State's international relations more broadly
  - E.g.: trade ties; membership in intergovernmental organizations; international law enforcement cooperation; treaty obligations
- Domestic factors relevant to state stability
  - E.g.: governing capacity; economic activity; development; public services; civil society; standard of living
- State capacity to deter and respond to security threats
  - For US and other countries, e.g.: critical infrastructure protection; counter terror; cyber security.

## Structure of this Report

In the process of collecting and coding the information contained in the US-DiGIA Directory itself, we realized that, as well as providing a resource tool for SOCOM, the directory itself could be analyzed to provide an overview of the USG discoverable information terrain. This report presents some of the key findings of our analysis of the directory. Part I explores the US-DiGIA Directory as a whole. Part 2 focuses on the subset of information assets relevant to gray zone challenges. This second part addresses Gen Votel's Task F to:

> Explore the nature of the capabilities (conceptual, procedural, and physical) necessary for navigating the gray zone successfully

Part 2 also demonstrates how tailored coding for specific issues or security concerns can increase the utility of the US-DiGIA directory for users with specific information needs.

To structure the following discussion of the descriptive statistics of USG discoverable information assets contained in the US-DiGIA, we organized the analytic narrative in each part around the three foundational whole-of-government questions that guided the structure of the directory itself.

1. *What* national security and foreign policy related information does the USG currently collect and hold?
2. *Who* (which organizations) collects and holds that information?
3. *Where* geographically are our information assets focused?

# Part I: Mapping the National Security Discoverable Information Terrain

Part 1 of the report explores the US-DiGIA directory as a whole, providing an overview of the range and sources of information assets held within the USG executive branch relevant to national security and foreign policy, as well as possible points of contact for interagency collaboration beyond the "usual suspects." Before moving on, however, it is important to remind readers that the US-DiGIA directory only includes *discoverable* information, not the complete information assets of the USG. This external limitation is particularly important to keep in mind when considering sensitive information categories such as intelligence.

## Topical Distribution of Discoverable Information Assets (the "What")

In recent years, changes in the nature of national security threats, such as the rise of violent extremism and cyber attacks, has broadened the scope of information planners and analysts need to consider to both predict and respond to threats. The growing emphasis on increasing our understanding of the human domain similarly increases information needs. In many cases, this pushes military planners and analysts to consider factors outside traditional military areas of expertise. Access to existing information assets can lessen the growing burden of information collection, while source organizations can potentially provide contextual background critical for interpreting and using such information.

Figure 2 below maps the distribution of all US-DiGIA information assets by DIMEFIL-plus categories. Discussing each of these in detail is beyond the scope of this report, but we have drilled down into some of the more complex or dominant categories to provide more detail.

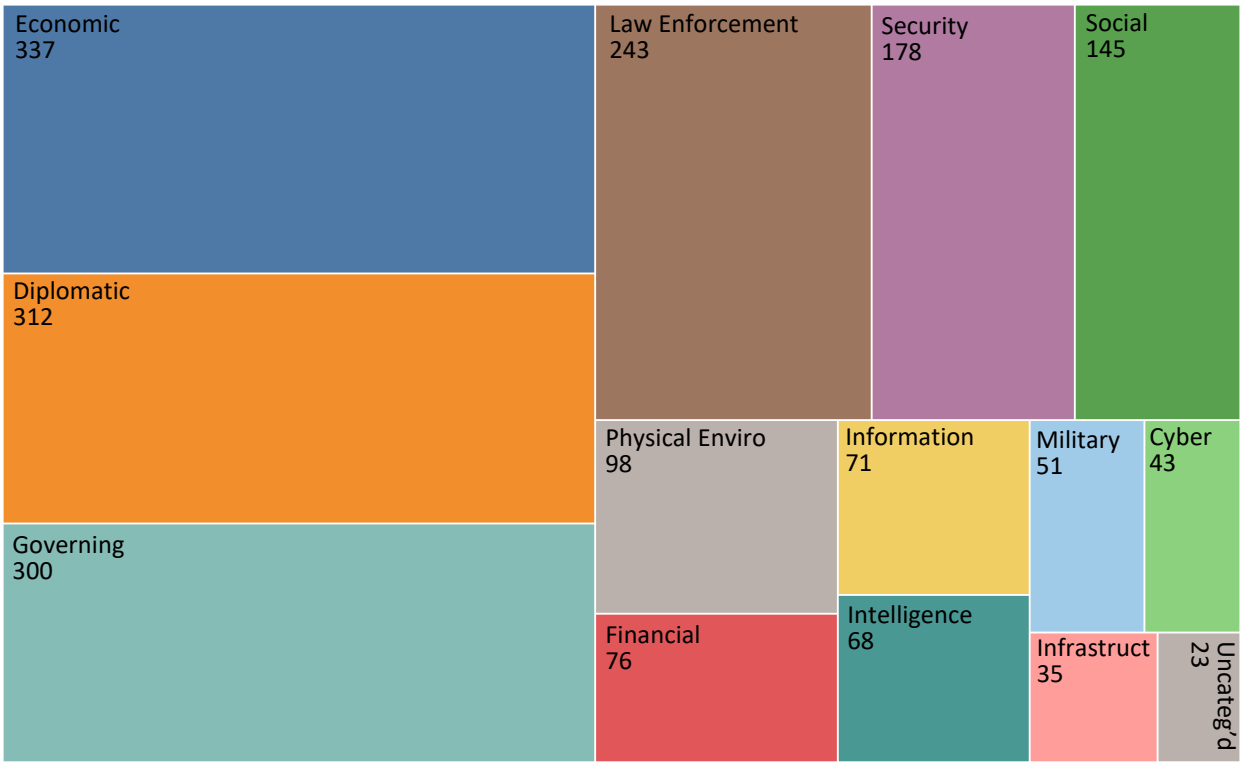



Figure 2: Distribution of Information Assets by DIMEFIL-plus Categories

## Diplomatic Information Assets

*Trade and security are the substantive focus of the majority of discoverable diplomatic information assets.*

Diplomatic assets reflect three broad areas of focus: trade and finance (25%); security (31%); and humanitarian (15%) issues (including global health and human rights). There are also a few that focus on scientific cooperation (2%) and the environment (3%). A good proportion of assets (24%) are devoted to the functional ways in which the US communicates and cooperates with other states (such as diplomatic representation, bilateral partnerships, and strategic communication).

## Economic Information Assets

*When it comes to economic aspects of national security and foreign policy, the information assets identified are US-centric and focused on trade.*

*We have more discoverable information assets related to economic issues than we do security issues.*

Breaking out the economic category (Figure 3), we see the size of the economic category is driven in large part by the quantity of information we have concerning US trade and international markets. Trade-related information accounts for 40% of information assets dealing with international economics and is distributed within 30 offices across four departments and three agencies. Energy and development-related information also accounts for a significant proportion (12% and 10%, respectively) of assets.

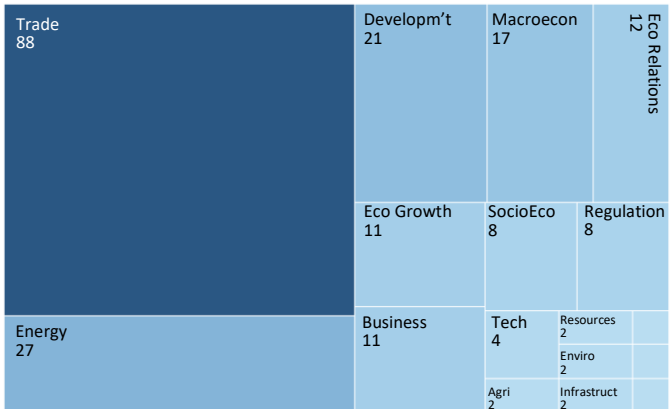


Figure 3: Distribution of Economic Information Assets

By comparison, there are far fewer information assets related to the regulation and governance of economic behavior. We identified only one office, the Office of Economic Policy Analysis and Public Diplomacy in the Department of State, that dealt with economic corruption and only five organizations that indicated they held information assets relevant to economic regulations (Depts. Commerce and State, DHS, USAID, and the US Trade Representative).

As discussed above, trade information related to international economic cooperation was coded into the diplomatic category not the economic category. Such topics account for a considerable proportion (25%) of the international diplomatic information assets identified across seven USG organizations. This further emphasizes the prevalence of economic information assets – in particular trade – compared to other foreign policy areas. When accounting for economically focused diplomatic information assets, economic-focused information assets account for 21% of all US-DiGIA assets, whereas those focused on security account for 14%.

## Cyber Information Assets

*While more organizations hold cyber related information than economic information, only three have a clear international focus to their cyber efforts.*

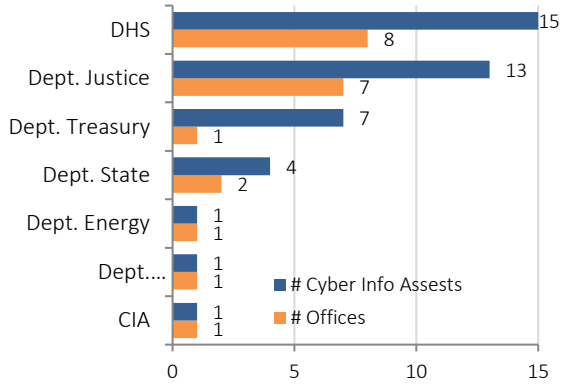



Figure 4: Distribution of Cyber Information Assets

Moving to the cyber category, we see from Figure 4 that comparatively fewer cyber related discoverable information assets were identified. Furthermore, when we look at the geographic coverage of cyber assets, we find that only CIA, Dept. Justice, and Dept. State have a clear international focus to their cyber efforts. There are several possible explanations for this. It could be a result of the coding; DIMEFIL-plus categories are not all equal in breadth (economic, for example, encompasses more topics than do either cyber or information). Alternatively, this relative scarcity of discoverable information assets may be a result of the more sensitive nature of some aspects of cyber—which would result in less detailed information being supplied by USG organizations on their work in this area. Finally, this variation could reflect the relative newness of cyber as an area of interests. However, this final explanation appears to be contradicted by the fact that cyber related assets are held by multiple organizations, and in many instances multiple offices within those organizations. More organizations address cyber issues than economic issues, highlighting the cross-domain nature of this specific issue.

## Social Information Assets

*Coverage of social information assets accounts for less than 10% of all discoverable information assets. Only a minority of this focuses on topics that can be directly linked to political stability.*

There is increasing attention being paid to the role of the human (inclusive of cognitive) domain in national security and foreign policy. To capture this concept we added a broad "social" category to the DIMEFIL-plus coding. Looking at the overall number of information assets in the social category (see Figure 2 above), it appears as though there is fairly substantial coverage of social factors (59 assets for the US and 86 international). However, breaking this category into component information classes (Figure 5) reveals that information assets in this category area are unevenly distributed. For example, information related to

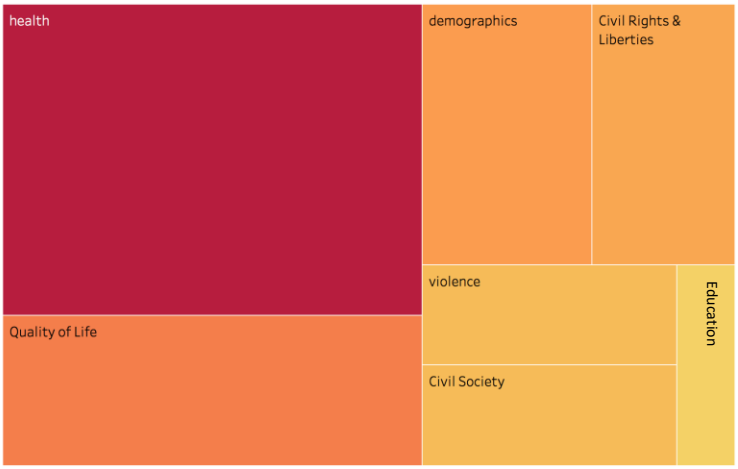



Figure 5: Distribution of Social Information Assets

health (in particular, disease) accounts for over a third (39%) of social information assets. Information assets that may have more direct bearing on aspects of the social domain that more directly influence state stability, such as civil rights and civil liberties (11%), civil society (8%) and violence (8%) are less numerous.

## Organizational Distribution of Discoverable Information Assets (The "Who")

One of the challenges in effectively utilizing the existing discoverable information assets held by the USG is determining which specific offices, in which organizations, hold that information. Not only is this critical for efficiently locating information, it can also provide a guide for identifying potential points for interagency cooperation. As Figure 6 below shows, of all USG organizations included in the US-DiGIA, the State Department has both the greatest quantity (501 information assets) and diversity (387 topics) of information relevant to national security and foreign policy. Other organizations, such as the US Trade Representative had a fairly large number of assets (117), but these were focused on a limited range of topics (29). Although the Departments of Health and Human services, Labor, Interior, and Energy all hold fewer overall assets, the assets that they do have cover a broader range of topics.

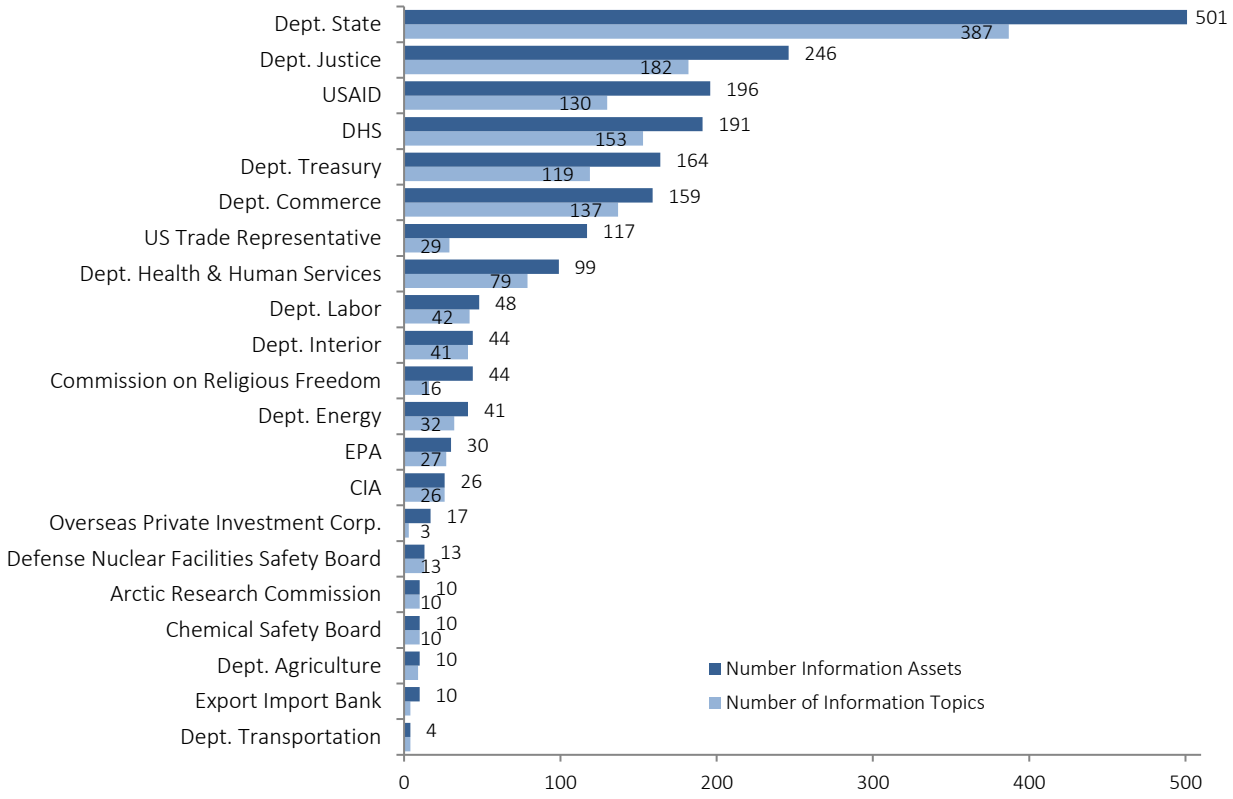



Figure 6: Distribution of Information Assets and Topics by Organization

The Department of Health and Human Services (DHHS) has a, perhaps surprising, number of relevant information assets (99). Many of these assets relate to disease detection and tracking or

emergency response and are primarily found in the CDC or the Office of Emergency Management, although six other DHHS offices were identified as having relevant information assets.

Also interesting to note, many organizations outside the intelligence community (IC), or the group of organizations that frequently coordinate with the DoD[1], were found to have information potentially relevant to national security and foreign policy. This finding provides support for the contention that we need to think more about whole of government when addressing national security and foreign policy issues. The types of discoverable information an office within an organization holds, provide an indication of the interests and expertise within that office. They can be used, therefore, to identify possible points for interagency cooperation. For large organizations such as the Departments of State and Justice, this can reduce the effort needed to locate appropriate contacts within the organization. For smaller and less familiar organizations, or those that may not have been known to hold relevant information, this directory provides the potential to broaden the scope of interagency cooperation beyond established collaboration paths.

## Geographic Distribution of Discoverable Information Assets (Where)

For some planning and analysis tasks, for example prevention of cyber attacks, the ability to locate information assets by topic (DIMEFILplus) is most helpful. In other cases, tasks may be focused on a specific country or geographic region. For this reason, we coded information assets according to their geographic coverage. As discussed in Appendix A, there is considerable variation in the specificity of the reported geographic scope of information assets. Adding to this difficulty, there does not appear to be a standard set of geographic regions employed by USG organizations. As a result of these variations in the precision with which we could identify the geographic focus of information assets, we consider geography at two levels: 1) a US/ international dichotomy[2]; and 2) where possible, a more specific coding by country or region.

### Domestic or International Focus

*Internationally focused discoverable information assets were more numerous than were US focused.*

Figure 7 below shows the distribution of information assets by DIMEFILplus and geographic focus. For the majority of DIMEFILplus categories, there were more information assets that were internationally focused than US focused. In some cases, such as diplomatic, this is a function of the category.

[1] From the organizations we examined, we coded the CIA and DHS as part of the IC and the Departments of State, Justice, and the Treasury as frequent coordinators.

[2] We coded an asset as US or country specific only in instances where the information was domestically focused. So, for example, trade topics are coded as international or for the region covered, rather than US, even if it relates to US trade.

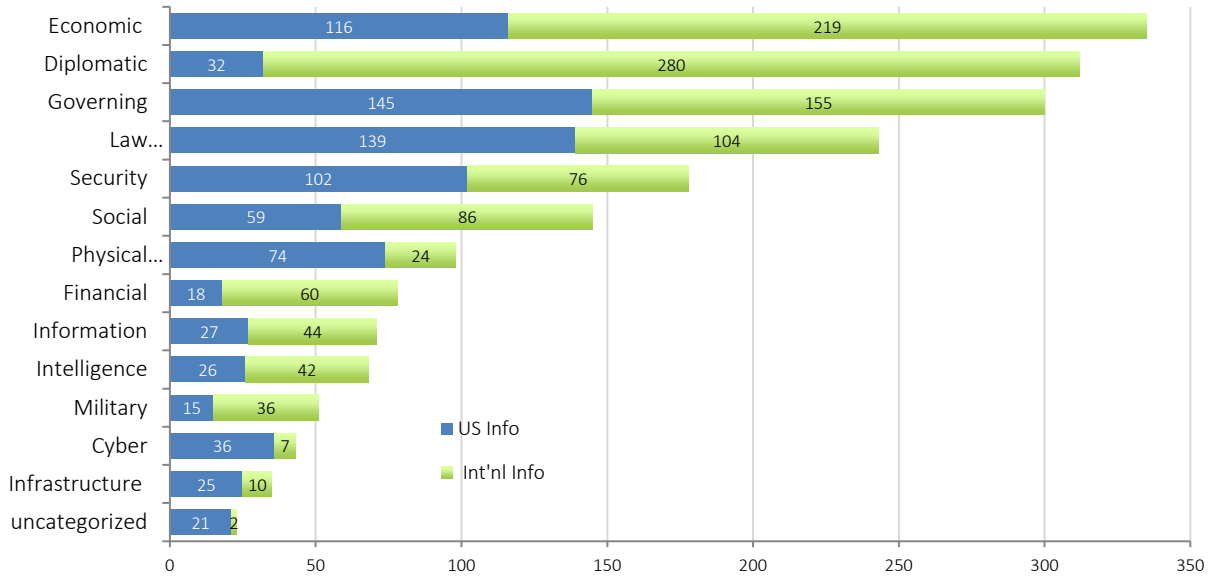



Figure 7: Distribution of Information Assets by DIMEFIL-plus and Geographic Focus (US/International)

Security is one category where a greater proportion of information assets relate to domestic US considerations. Looking at the information topics in this category, we see that this US weighting is driven in large part by information assets held by the Department of Homeland Security, in particular information topics related to counter-terrorism, terrorism preparedness, and border security. Not all counter terrorism and CVE information assets are primarily focused on the United States, however. The Departments of State and Justice have counter terrorism information assets as well, and many of these are outward facing, in particular those concerned with messaging, information sharing, international investigation, and capacity building.

Law enforcement is another category where the majority of information relates to domestic US considerations. The majority of international law enforcement information assets relate to drug trafficking, money laundering, and human trafficking. Physical environment information assets are both more numerous and more varied for the US than internationally, mainly driven by the wealth of data collected by the Department of the Interior. Finally, as discussed earlier, we found only 7 cyber related information assets that we could identify as internationally focused.

## CCMD AOR Specific Information Assets

*Many information assets are not clearly geographically defined, which creates inefficiencies when searching for country or region specific information. It also makes it harder to identify countries or regions where national security and foreign policy relevant information is lacking.*

Figure 8[3] below shows the distribution of geographically specific information assets related to each CCMD AOR. It is important to remember that here we are looking at a subset only 349 information assets, so any conclusions we make regarding the depth and breadth of information available for a specific CCMD is highly contingent.

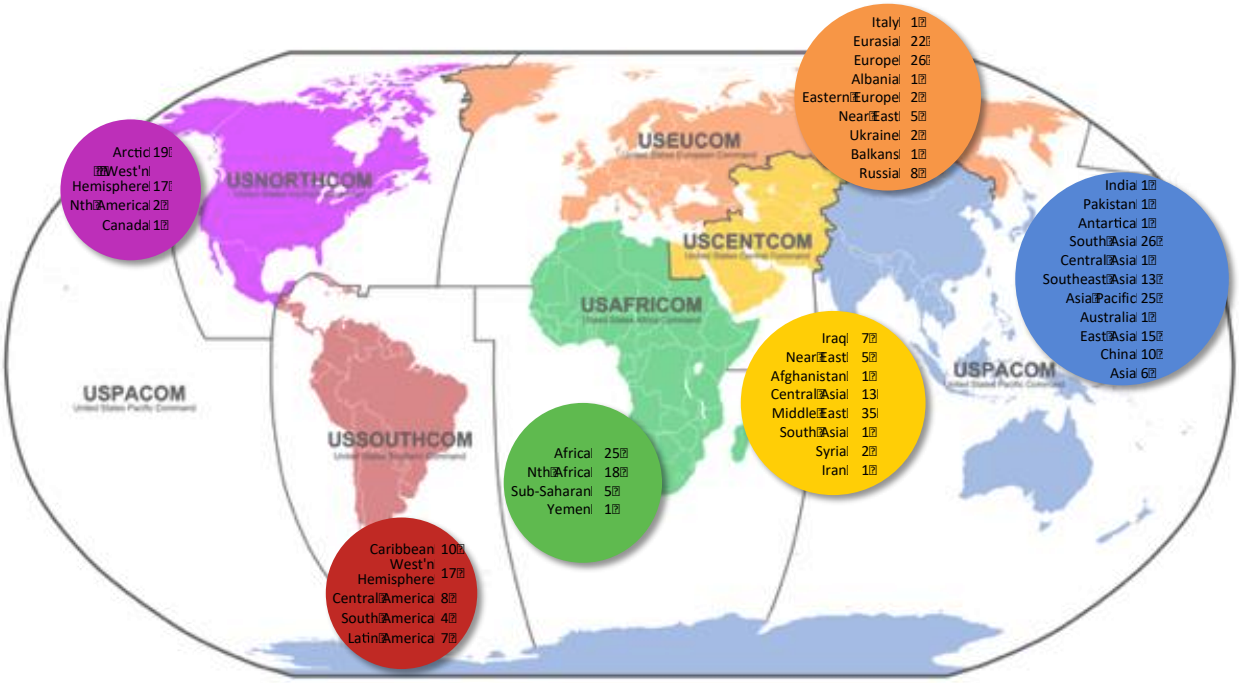



Figure 8: Distribution of Discoverable Information Assets by Geographic Coverage

We were able to identify more information assets specific to PACOM than to other CCMDs. PACOM AOR-specific information assets account for 25% of all geographically specified assets, across more organizations (three departments and five agencies) and offices (16) than any other CCMD. We found the fewest number of offices specifying information relevant to the AFRICOM (10 offices) and SOUTHCOM (8 offices) AORs. We also found variation in the coverage of countries and regions within specific CCMDs. For example, almost half (49%) of information assets related to NORTHCOM's AOR deal with the Arctic, whereas we identified only one asset specific to Canada. Given the current salience of Arctic issues, this concentration could be beneficial to planners and analysts. Among the specific information topics identified for the Arctic are economic potential, ship

[3] CCMD map source: By Lencer - "own work", neu erstellt unter Verwendung von BlankMap-World6.svgQuelle: USAFRICOM United States Africa Command Map Draft und Unified Command map, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=2774840

access, energy and infrastructure development, and information regarding the physical environment—all of which could provide useful insights.

### Distribution of CCMD AOR Specific Information Assets by DIMEFIL-plus

We can also consider variations in discoverable information assets across the CCMDs by considering the distribution of DIMEFIL-plus categories for each CCMD. A graphic illustration of this is presented in Figure 9 below.

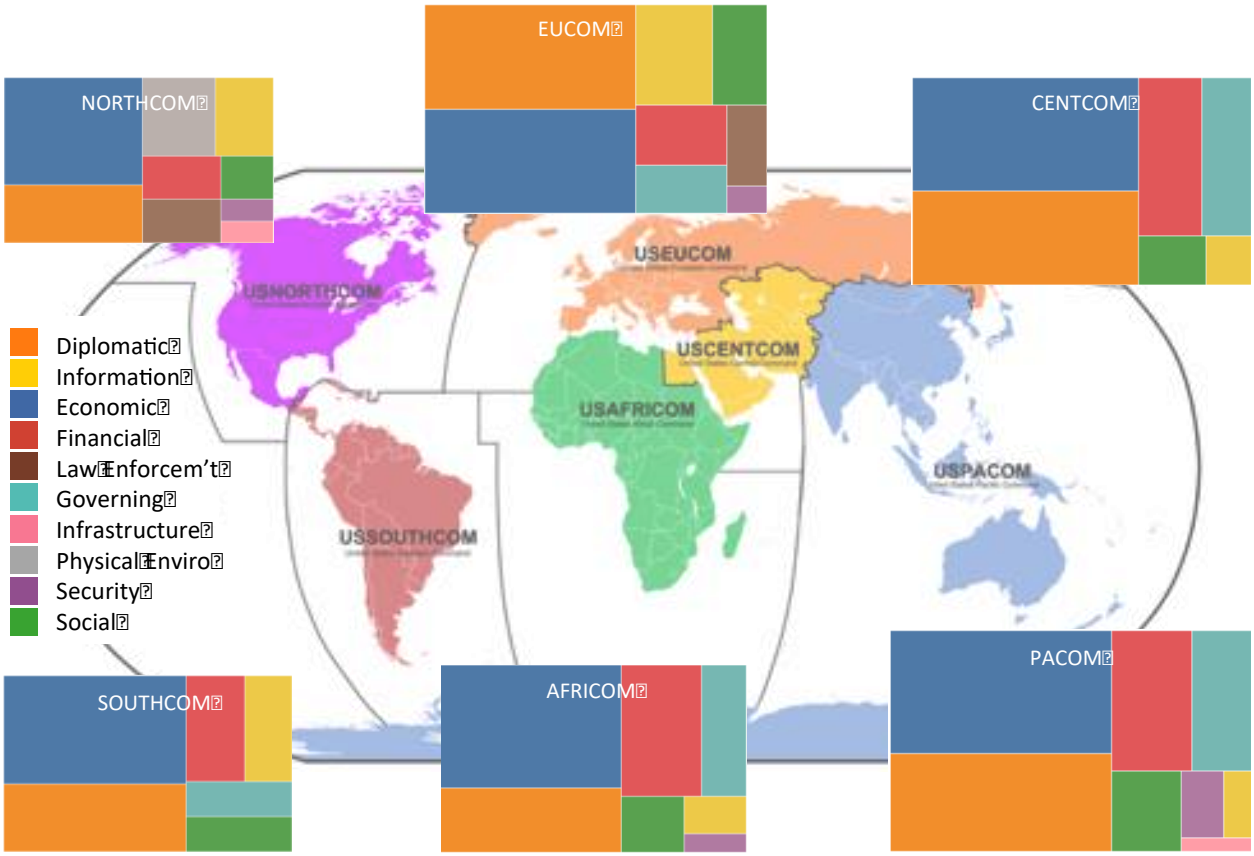



Figure 9: Distribution of Information Assets Across CCMDs by DIMEFIL-plus

For all CCMDs, economic information was the most common, then diplomatic. This finding is consistent with, and reflects, the distribution of the full US-DiGIA (see Figure 2 above). Also, consistent with the general pattern observed, it is notable that we identified no geographically specified information assets related to intelligence military, or cyber. Again, this is not to say that such information is not available, but rather that this information was not discoverable.

## Part II: Mapping the Gray Zone Discoverable Information Terrain

The gray zone is a conceptual space between peace and war, occurring when actors purposefully use single or multiple elements of power to achieve political-security objectives. Successfully navigating this space, therefore, requires military planners and analysts to think across a broad range of domains, some of which will be less familiar to them. Part of this navigation will also require coordination with other branches of the United States government to identify the capabilities the US possesses to identify and respond effectively to gray zone challenges. As Gen. Votel's tasking implicitly acknowledges, gray zone challenges epitomize the recognized need for a whole of government approach to national security challenges.

In order to directly address Gen Votel's Task F (Explore the nature of the capabilities—conceptual, procedural, and physical—necessary for navigating the gray zone successfully), the NSI team tailored the US-DiGIA Directory to identify information topics relevant to gray zone challenges. To provide the greatest utility for analysts, we needed to develop a coding scheme that not only identified whether a specific information topic was gray zone-relevant, but how. We approached this task by returning to the SMA definition.

As Figure 10 below illustrates, we grouped the gray zone relevant information topics into 148 broader information elements, which were in turn rolled up into 31 information classes. Finally, these classes were coded to the four gray zone dimensions derived from the SMA definition: action, actor, international rules and norms, and US interests and capabilities.

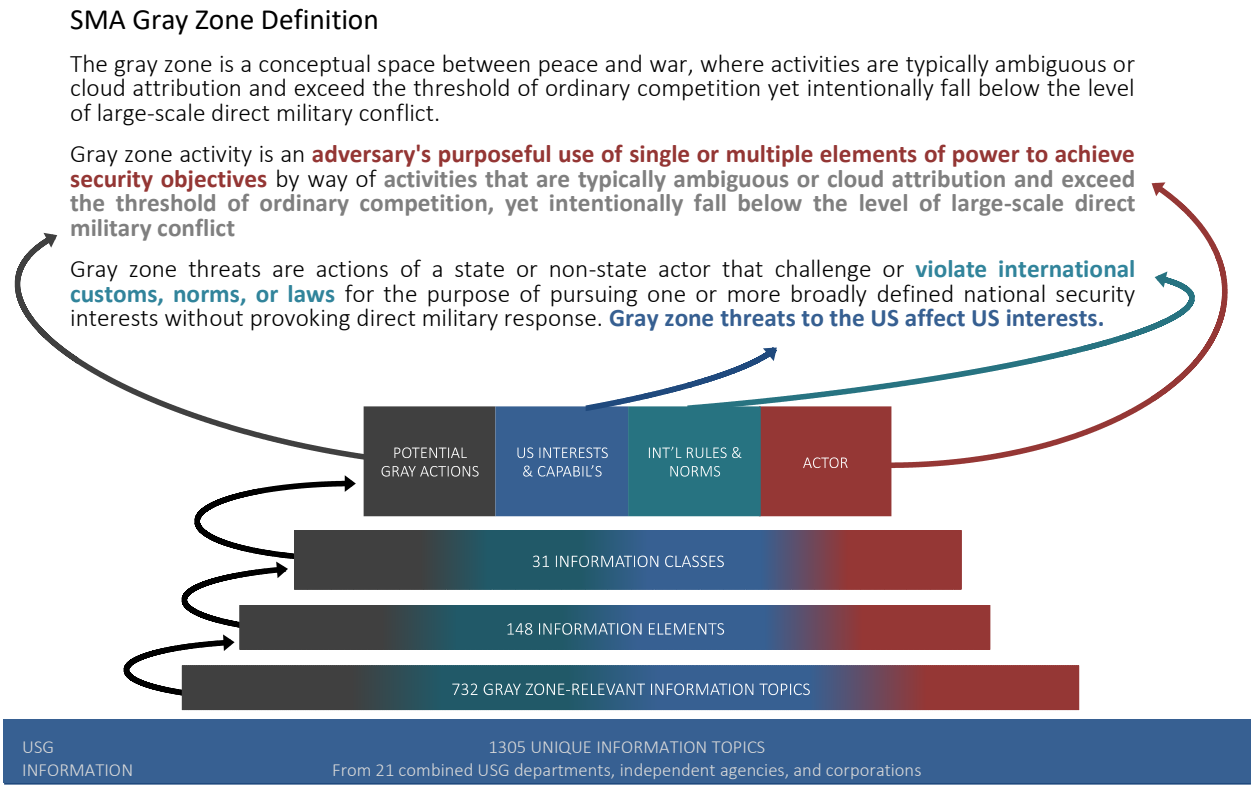



Figure 10: Gray Zone Coding Scheme for US-DiGIA

Developing this coding scheme[4] revealed that some elements (e.g., cyber espionage) are relevant to more than one gray zone class (in the case of cyber espionage: political influence and destabilization, economic coercion and sabotage, corporate espionage, and cyber attacks). To preserve the complexity of the various elements that compose classes, we thus allowed for double coding of some information elements—which needs to be kept in mind when reviewing information summaries. [5] As a result, the counts of information assets in this section of the report should be considered only at the class level. The totals across classes are inflated due to the nature of the coding.

## Overview: Information at the Gray Zone Dimension Level

### What do we Know? Distribution of Gray-Relevant Information Assets by Gray Zone Dimension

*While we have considerable information about US interests, we have few assets that can inform our understanding of international rules and norms.*

Figure 11 shows the distribution of information assets by the four gray zone dimensions (US interests; potential gray actions; actors; international rules and norms). There are more discoverable information assets connected to US interests than to other dimensions. Information assets related to International Rules and Norms, on the other hand, are relatively scarce. Given the importance of norms to understanding gray challenges, this gap could prove an impediment to both identifying and countering gray actions. We will return to this issue in a later section of the report (Looking Deeper: Distribution of Information at the Gray Zone Class Level).

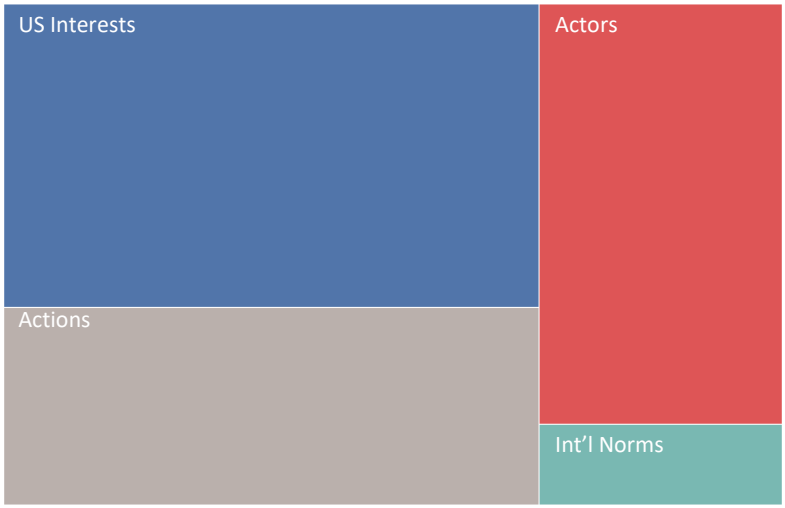



Figure 11: Proportional Distribution of Information Assets by Gray Zone Dimension

[4] As the SMA Gray Zone effort is focused on gray challenges to the US, we reference here the earlier version of the SMA definition that specifies threats to US interests.
[5] A full list of the information dimensions, classes, and elements can be found on the "Gray Zone Coding Scheme" tab of the US-DiGIA Directory.

## Who Holds that Information? Distribution of Gray-Relevant Information Assets Across USG Organizations

*Gray zone relevant information is widely found in organizations beyond the "usual suspects" (those with a security or IC focus), underscoring the need for a whole of government approach to effectively address gray zone challenges.*

As Figure  below shows, we identified gray-relevant information assets within all but two (Chemical Safety Board, Defense Nuclear Facilities Safety Board) of the organizations examined. The fact that the Department of State holds the largest number of gray-relevant information assets is likely unsurprising given both the size and mission of the Department. However, a rich supply of information assets can be found in other organizations. For example, despite being either primarily domestically focused or without a direct security mission, we found gray-relevant information assets are held by the Commission on Religious Freedom (e.g.: religious violence; human rights), and the Departments of Labor (e.g.:  international labor laws), the Interior (e.g.: energy infrastructure; offshore energy rights), and Agriculture (e.g.: food safety).

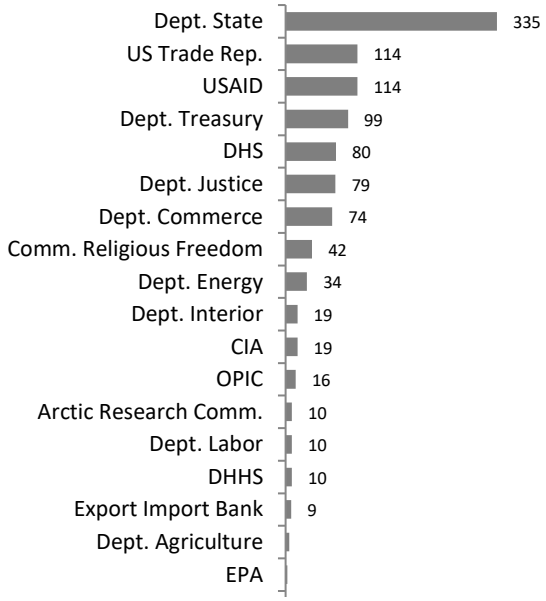



Figure 12: Distribution by Organization of Gray Zone Relevant Information Assets

This distribution of gray-relevant information reflects the fact that actors operating in the gray zone can and do utilize multiple elements of power. Gray actions can take place in the economic, political, and social realms, as well as more traditional military spheres. Identifying and responding to gray challenges efficiently and effectively *requires* information across all these domains and the contextual understanding of them to more accurately determine attribution and intent.

Consequently, identifying and mitigating the negative consequences of gray zone challenges necessitates whole of government approaches. In particular, better and more regular interagency cooperation may allow for the information assets and expertise relevant to developing indicators and warnings of gray activity already present within the USG to be leveraged by planners and responders for more effective, multi-faceted responses. Increased information and expertise sharing across government offices also means that the practitioners who best understand specific instruments of power can be involved in their application to specific gray zone challenges. Similarly, greater interagency cooperation may, by bringing diverse areas of expertise and authorities together, create the potential for developing earlier and more sensitive indicators and warning and a broader and more adaptive set of strategies for countering such threats.

## Who Knows What? Distribution of Gray-Relevant Information Assets by Organization and Gray Zone Dimension

*Organizations outside the IC hold information assets relevant to all gray dimensions. There is a greater diversity of USG organizations collecting and holding information assets relevant to actors and US interests than gray actions or international rules and norms.*

When we break out the distribution of the organizations' information assets by gray zone dimension (Figure 13below), we can see that, with the exception of the US interests category, the Department of State remains the dominant source of information. We found information assets relevant to both US interests and actors in more organizations (18) than we did information assets associated with actions or international rules and norms (12). Combined with the number of information assets, this makes US interests the gray dimension where the USG has the greatest depth and breadth of information. Information relating to international rules and norms, on the other hand, not only generated fewer information assets across fewer organizations, but the majority of the discoverable assets are held by only two departments—State (45% of total assets) and Treasury (22% of total assets).

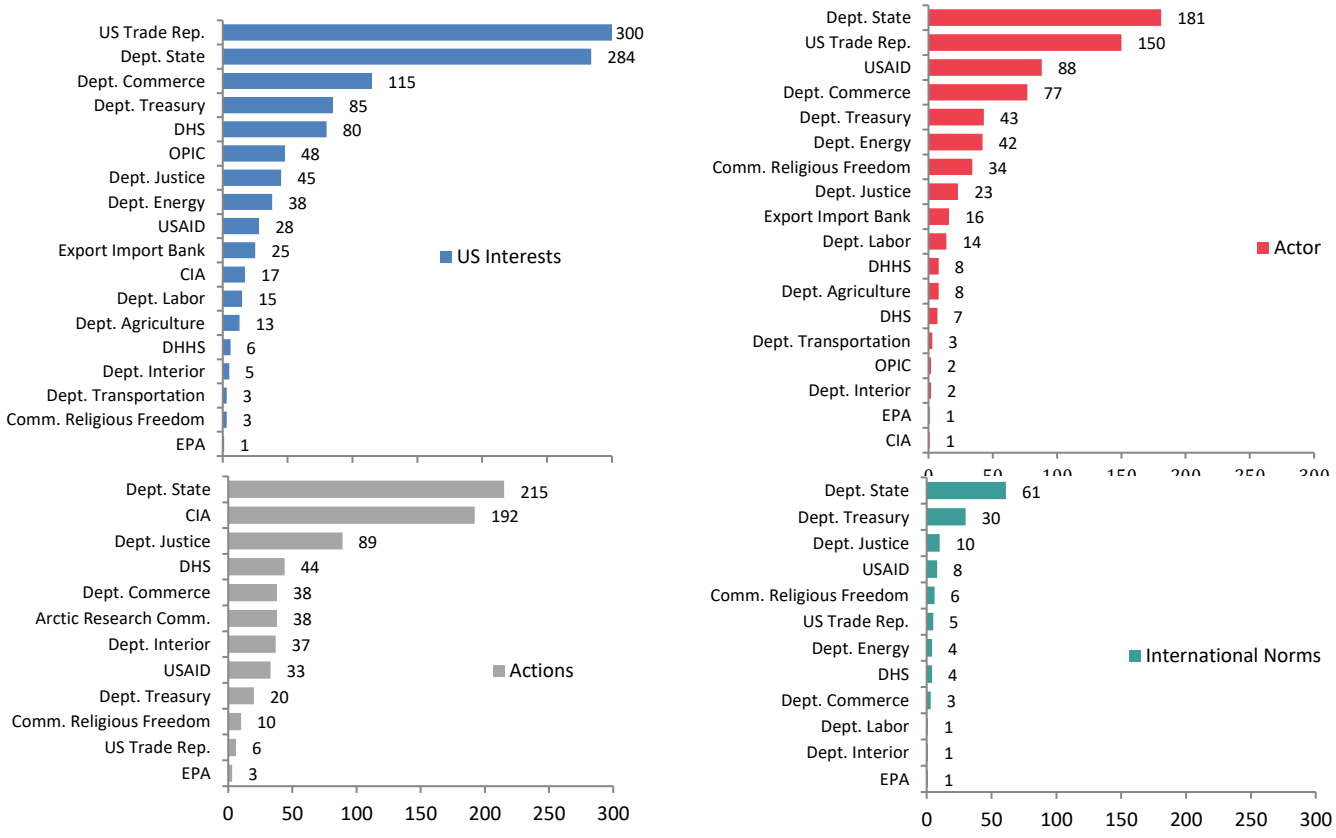



Figure 13: Distribution of Information Assets by Gray Dimension and Organization

## Where is Our Information Focused? Geographic Distribution of Gray Zone Information Assets

*Identifying which information assets cover specific CCMD AORs is in many cases not possible from the published descriptions. This creates inefficiencies when searching for country or region specific information, and it makes it harder to identify countries or regions where gray zone relevant information is lacking.*

As with the US-DiGIA as a whole, we were also interested in getting a sense of how gray-relevant information assets were distributed geographically. To do this, we followed the same approach as in part one. First, as shown in Figure  below, we used a dichotomous US/international coding. At this level of detail, we find that the State Department, US Trade Representative, USAID, and Treasury all have more gray-relevant information that is internationally focused rather than domestically focused. Given their missions and authorities this is to be expected.

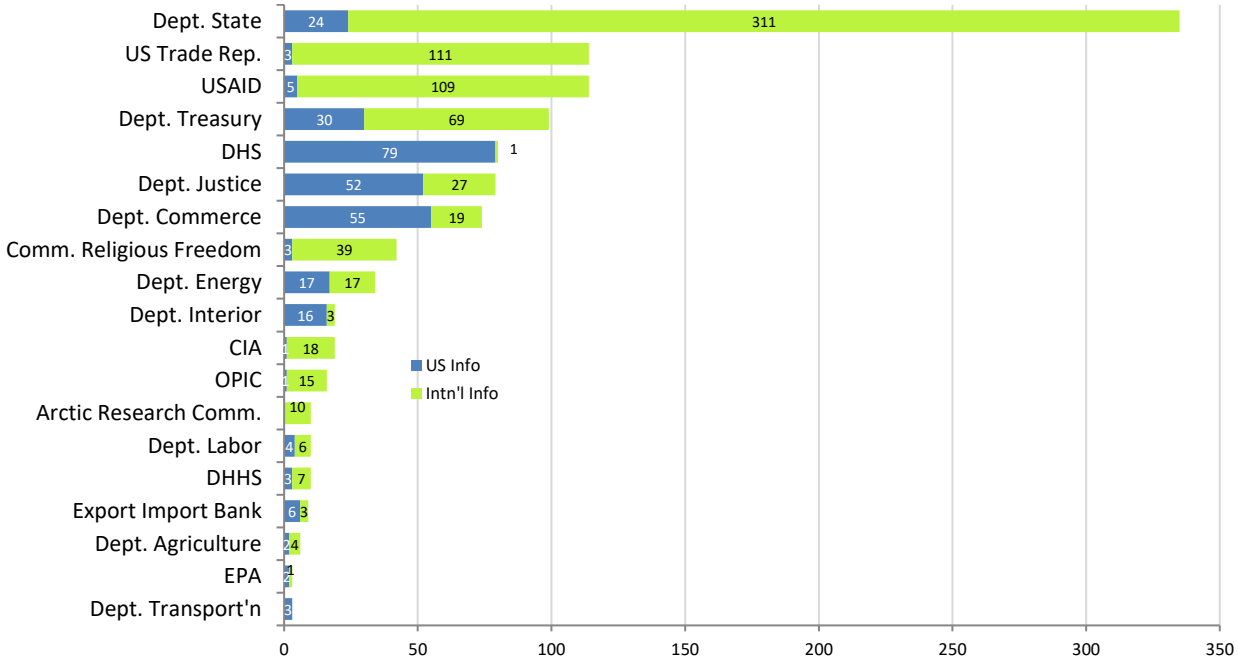



Figure 14: Distribution of Gray-Relevant Information by Department and Geographic Focus

What is perhaps less expected is the proportion of gray-relevant information in the DHHS, Department of Agriculture, and Department of Labor that is international in focus. For the DHHS, much of this is information related to health care capacity building and standards. In the Department of Agriculture, international information relates to agricultural trade, and the Department of Labor's international information is divided between labor statistics and laws and trade agreements. This finding once again points to the potential benefits to analysts and planners of looking beyond those USG organizations outside the IC or the group of organizations that frequently coordinate with the DoD when seeking information relevant to addressing gray zone challenges.

### *Distribution of Gray-Relevant Information by CCMD AOR and Gray Dimension*

For some of the information assets, we were able to identify a more specific (country or region) geographic focus, and we coded this subset of the data to the relevant CCMDs. Figure  below shows the distribution of these information assets for each CCMD AOR, specified for the gray zone dimensions.

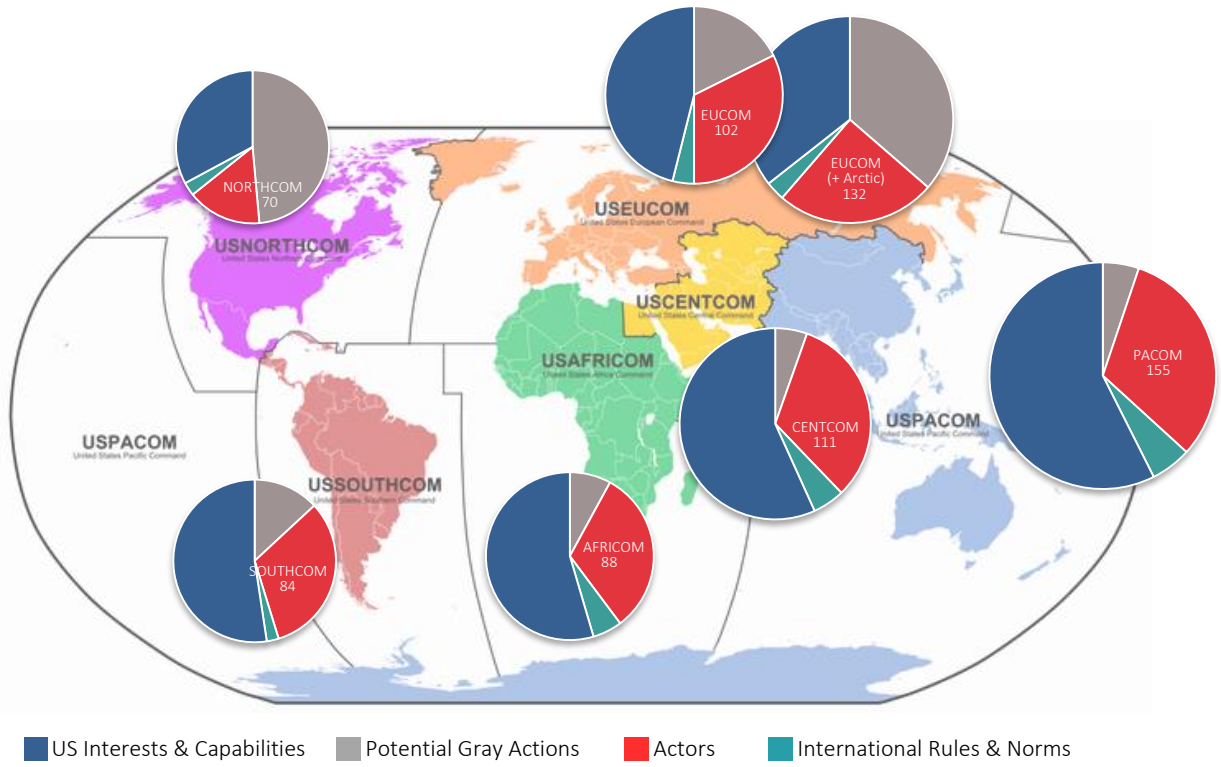



Figure 15: Distribution of Geographically Specified Gray-Relevant Information by CCMD AOR

Overall, the trends found in the general US-DiGIA hold for the gray zone relevant subset. We found more information specified for PACOM, CENTCOM, and EUCOM AORs than for the other CCMDs. For SOUTHCOM, NORTHCOM, and AFRICOM, the distribution of information assets by gray zone dimension mimics the distribution for the gray zone US-DiGIA as a whole (see Figure 11). That is, for these CCMDs, we know most about US interests and least about international rules and norms.

There is, however, some variation in the distribution of information assets by gray zone dimension across the various CCMD AORs. This is seen most clearly in the case of the action dimension, which accounts for a greater proportion of EUCOM, NORTHCOM, and SOUTHCOM AOR-specific information assets. For EUCOM and NORTHCOM, this variation is driven by information assets specific to the Arctic, an area that has recently generated considerable interest and concern. The Arctic, as a geographic region, was a difficult case to categorize properly for the purposes of generating summary data. While NORTHCOM has been designated as the lead geographic command for developing and advocating for US Arctic interests, six of the eight states with territory

within the Arctic Circle are within EUCOM's AOR. More importantly, EUCOM engages with these states as well. As many of the gray zone Arctic information assets relate to gray actions, these drive the higher overall proportion of Action assets we see in both the NORTHCOM and EUCOM distributions. For SOUTHCOM, action information types reflect a topical rather than geographic focus, with all but one related to political influence and destabilization or propaganda and information campaigns.

## Looking Deeper: Distribution of Information within Gray Zone Dimensions

While the broad categories of the four gray zone dimensions are helpful for a bird's eye view of the distribution of discoverable information assets, it is also helpful to conduct a more granular analysis of gray-zone relevant discoverable information. In order to do this, we analyzed summary data pertaining to the 33 gray zone classes. Figure  below shows the distribution, by gray zone class, of gray relevant information assets for each gray zone dimension.

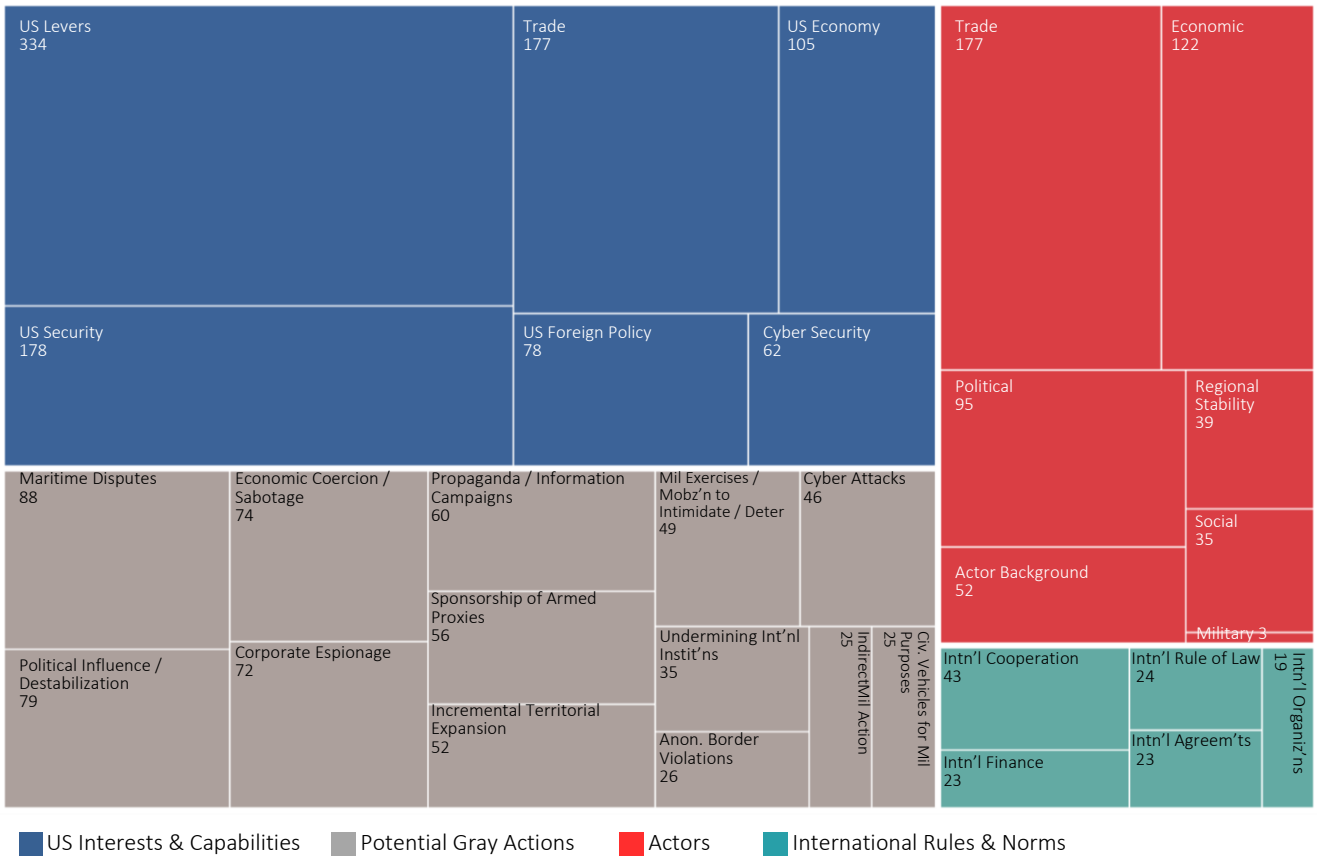



Figure 16: Distribution of Information Assets within Gray Zone Dimensions

## Information Assets Relevant to US Interests & Capabilities

*USG agencies collect and hold considerable information about US economic activity and relations. Better understanding of these economic relationships may help identify where and how US economic levers can be employed to counterbalance the use of economically focused gray actions by others.*

The US interests (blue section of Figure  above) class for which we identified the most information assets was *US levers*. This class is designed to capture information relevant to the elements of power and influence that the US can bring to bear to either respond to or deter gray zone challenges, or to engage in its own gray actions. Included in this class are:

- Economic levers (such as foreign assistance—military and humanitarian, foreign investment, trade)
- Diplomatic and political levers (e.g., strategic communication and public diplomacy)
- Military levers (e.g., military to military cooperation, military assistance, and security cooperation)

Overall, we see a definite skew in the US interests information toward economic information. Not only is a considerable proportion of the *US levers* class economic in nature, the classes with the third and fourth most discoverable information assets are *US trade* and *US economy*. As discussed in part one of this report, this finding may be partly an artifact of the nature of economic activity and information. Economic information is both amenable to quantification and less sensitive than other gray relevant information, therefore it is more likely to be identifiable through the data collection method we used for US-DiGIA. However, the finding could also reflect an inherent bias in the manner in which the US prioritizes information acquisition. That is, we engage with the world most extensively through economic ties, and consequently value economic information, which is also simpler in many cases to collect and quantify than information relevant to other gray dimensions.

We have seen how effectively states, such as Russia, can use economic power as one element of gray strategy (most clearly in the disruption of gas supplies to Ukraine following the 2013 Maidan protests). The economic and political structure of the US does not provide the US government with the same capacity to manipulate economic activity that governments such as Russia and China possess. As we see in the Asia Pacific region and Eastern Europe, smaller states face potentially painful and domestically destabilizing consequences for confronting an aggressive or expansionist power on whom they are economically dependent. However, understanding and accounting for economic relationships may help us to better determine intent, recognize vulnerabilities in other actors, and potentially reduce these vulnerabilities through the application of our own economic soft power.

## Information Assets Relevant to Actors

*There is a growing recognition that identifying and countering gray zone strategies requires an understanding of the motivations of gray actors as well as the vulnerabilities of their targets. However, discoverable information for the actor dimension is relatively scarce, particularly information that could provide insight into the perceptions and attitudes of foreign leaders and populations.*

The actor dimension of the gray zone coding scheme (red section of Figure above) captures information about actors other than the US—both potential gray actors and targets of potential gray actions. As potential gray actions may involve the use of economic, political, or social elements of power as well as military actions, the range of information included in the actor dimension was correspondingly broad. In addition, in order to capture more contextual information that may provide indications of an actor's propensity to engage in gray activity, or their vulnerability to such actions by others, the NSI team also included information relevant to regional stability and an actor background class. The latter is designed to identify more general information and subject matter expertise that may help analysts identify the interests, constraints, and goals of a specific actor.

Looking at the distribution of information assets by actor classes, we see that, even more so than for the US, the weight of the discoverable information assets is in economic and trade data (43%), and both these classes also have greater diversity of information assets (20 information elements) than other actor classes. We identified a variety of information assets for the political class, across a broader range of 12 elements, including government capacity and performance, and political process.

Only 5% of the discoverable information assets in the actor dimension are related to social factors. The social elements for which we discovered information assets are: civil conflict; civil society; demographics; food security; poverty; and water security. While these elements can all potentially provide insight, particularly into a state's vulnerability to gray actions, alone they cannot provide the information necessary to provide a comprehensive picture of the social context of a specific state.

This gap in social information assets is relevant not only to gray zone challenges but to US security and engagement activities more generally. We recognize that there is a wealth of information in the form of informal institutional and SME knowledge within various government organizations that could mitigate this deficit. However, if others have no way of identifying who may hold such information, this rich source of additional information will remain a non-transferable resource.

## Information Assets Relevant to Gray Actions

*We found few information assets that could be directly used as indicators and warnings of gray actions. However, we did identify information assets that could be useful for determining an actor's vulnerability to gray actions and physical environment data that may contribute to identifying areas of potential gray conflict.*

As the SMA gray zone effort has emphasized at multiple points, one of the challenges associated with identifying and planning for gray actions is that there is no single condition that can identify an action as gray, regardless of actor or context. The nature of the action, intent, and context must all be taken into consideration when determining whether a specific action (or set of actions) is gray or not. That being said, actions are a critical component of the gray zone definition. Consequently, information regarding specific actions that *may* be gray is essential to the development of indicators and warnings.

We therefore took a deductive approach to coding the action dimension (gray section of Figure ), compiling a list of the specific (e.g., Chinese island building in the South China Sea) examples cited

by the COI as gray. To this we added the more general actions and activities referenced and discussed (e.g., cyber attacks; interference in the domestic political process of other actors). This gave us a set of thirteen generalizable classes of gray actions and identified the gray elements that would be relevant to the development of indicators and warnings. This current coding of action is not, therefore, definitive or final. Rather, it captures the current thinking on the scope of potential gray actions the US may face.

Again, the dominance of economic information assets is apparent in the action dimension, with economic coercion and corporate espionage in the top four categories for information assets. We found the greatest number of information assets for the maritime dispute class of action, but this is strongly driven by the inclusion of information related to the Arctic (19 assets).

For political influence / destabilization and propaganda / information campaigns, we identified a range of information elements. However, most of these are more relevant to determining the potential vulnerability of an actor to such gray strategies, rather than the direct identification of ongoing actions. For example, information regarding access to information and civil society can both provide context for understanding population vulnerabilities to external manipulation, and corruption information can indicate the ease with which political influence may be exerted over political decision makers.

One gray zone element for which there are significant information assets is *physical environment data*. This information element encompasses all data (such as weather, energy and water resource, marine, geological, and satellite) related to the physical environment and is held by the Departments of Commerce, the Interior, and State, as well as USAID and the EPA. Not all of the topics classified under the physical environment data element will be relevant to all Action classes; however, the salience of energy and resource issues to current conflict and competition within the international system suggests that this information could contribute to identifying areas of potential gray conflict.

### Information Assets Relevant to International Rules and Norms

*We have few specific information assets that help explain the informal relationships and practices that undergird formal international law and obligations. Norms violations are a critical component of gray actions, and this informational gap puts the US at a disadvantage.*

There is a building consensus that international norms violations are a distinct and central element of gray actions and strategies. This is the gray dimension, however, for which we identified the fewest information assets. Furthermore, the majority of this information is formal and procedural in nature; lists of international agreements to which the US is party and their obligations. The international cooperation class does touch on some areas of norms development, specifically Internet governance, and space cooperation. However, we were not able to identify any information assets that capture the role that norms play in supporting international law or would clearly provide an overview of prevailing international norms. As with the actor background class discussed above, this finding may be partly a function of the nature of the concept we are trying to capture. We are trying to identify contextual, qualitative understanding of the informal practices that govern relations between actors in the international arena, and this is something that we tend to do unconsciously, often recognizing its presence only when we experience violations of

expectation. We have no doubt that the US has many skilled and experienced personnel who hold knowledge valuable for building a picture of norms. However linking these experts within this domain to specific information topics using discoverable information currently poses a challenge. Either the discoverable information lacks specificity or the nature of the information itself is too general and conceptual ('fuzzy') to be easily referenced and thus made discoverable.

## Discussion

The US-DiGIA is a first step toward a directory of discoverable (unclassified, web-accessible) information assets relevant to national security and foreign policy, collected and held by USG organizations outside the DoD and ODNI. The full directory has been coded (using a DIMEFIL-plus approach) to help analysts and planners locate information relevant to a wide variety of national security questions and challenges. Organizations that frequently coordinate with the DoD and those that do not were both found to have information potentially relevant to national security and foreign policy. As discussed in Part II, the US-DiGIA can be further tailored to address a more specific area of concern—in this case gray zone challenges.

*The ability to identify and locate information assets across a broad range of USG organizations could reduce the need for SOCOM and others to undertake their own information collection. This in turn increases the efficiency of information collection and reduces cost in both time and resources.*

### Variations in Coverage Across the Information Terrain

Although we identified approximately 1,300 unique information topics, the distribution of that information, both topically and geographically, was not even. At this stage, we cannot determine the specific cause of the variations in coverage of the DIMEFIL-plus and gray zone information classes or geographic region. There are, however, several likely explanations for this:

#### Interest and Focus

First, and most simply, we pay more attention to things that are important to us, and the uneven distribution of information may reflect the fact that some topics are simply more salient to USG organizations than others. It is also possible that our information efforts lag behind changes in the domestic and international environment; we simply haven't thought to start collecting information on certain topics. This may particularly be the case when it comes to the gray-zone action categories, as many of the actions coded are either more recent phenomena (such as cyber attacks), or have only recently been considered within the US as strategically motivated activities (for example, economic coercion and sabotage).

*The current scarcity of information related to potential gray actions places the US at a disadvantage when it comes to developing indicators and warnings. These gaps highlight areas where SOCOM and others could focus their own information collection efforts to maximize efficiency and impact for analysts and planners.*

### Discoverability

As discussed in the body of the report, discoverability can be affected by the nature of the information, in particular its security sensitivity. As the US-DiGIA only catalogues unclassified and published information assets, it is to be expected that areas such as intelligence, cyber security, and political influence may be less represented not as a function of lack of interest or knowledge, but because of their sensitivity. In other words, it is the nature of the information itself, or the use to which we seek to put it, that limits discoverability.

Some topics, such as many in the social and actor categories, are more conceptual, dealing with factors such as perception and motivation. These topics are not as amenable to classification, given the degree to which they require interpretation and enumeration, unlike many economic factors. Such information is more likely to be held as institutional or SME knowledge; however, this is problematic in terms of information discovery and classification. There is an even greater gap for these types of topics when it comes to gray relevant information. Attribution and the determination of intent (motivation) can be critical in distinguishing between competition and gray conflict.

*Reaching out to organizations and requesting their direct assistance in identifying and coding their information assets would be a logical next step in increasing the depth of the current US-DiGIA.*

## Implications

Lack of information leaves us functionally blind to potential opportunities to further US interests, or mitigate threats to those interests. As the challenges facing the US in the international arena become both more diverse and more complex, analysts and planners increasingly need to consider situations that are beyond the domain of traditional military threats. This is particularly evident in the case of gray zone challenges that, by definition, utilize multiple levers of power. Without reliable information, it is more likely that we may incorrectly classify an action as gray, and increase the risk of either unintended escalation (by assuming an action is gray when it is not), or missing threats to our interests (by assessing an action as not gray when it is in fact gray).

Appreciation of the complexity of the evolving security environment has prompted calls for a whole of government approach to national security challenges. Information exchange is a logical first step in increasing awareness of common interests and information assets across the USG, and the US-DiGIA can contribute to that process. The types of discoverable information an office with an organization holds and also provides an indication of the interests and expertise within that office, and thus a guide to the identification of possible points for interagency cooperation. Interagency collaboration enables the practitioners who best understand specific instruments of power to be involved in their application to specific national security (including gray zone) challenges. Similarly, bringing diverse areas of expertise and authorities together can reduce institutional bias and reveal underlying assumptions. This can create the potential for developing a broader and more adaptive set of strategies for responding to gray zone and other national security threats, and avoiding unintended consequences.

## Appendix A: Scope and Limitations of the DiGIA Directory

The task of mapping the informational assets of the USG is, of course, a labyrinthine and potentially never ending task, as information acquisition and dissemination is a continuous process. For this project, therefore, we needed to find a systematic and logical way of bounding the search process. First, we focused on Executive Branch departments, agencies, and corporations outside the DoD and IC. Second, we drew on information that the organizations provided on their websites (hence the restriction to "discoverable" information).

Our mapping process involved taking unstructured information (e.g., mission statements, program descriptions, report abstracts, tools, and data sets) and converting it into data.[6] We found significant variation in the organization of websites, the amount and detail of information provided, and the frequency with which these websites were updated.[7] While this variation is to be expected, it does have significant implications for how we frame and understand the US-DiGIA directory and any analysis that we may conduct using its contents. In short, the US-DiGIA database should not be considered to be *the* final, comprehensive accounting of all the information assets held by the USG or the 21 organizations included.[8] Rather, the US-DiGIA captures the range of these organizations' discoverable national security/foreign policy related information assets.

The broad search parameters we used uncovered over 1,900 individual "pieces" of information (information assets) in various forms (e.g.: reports, data sets, SME knowledge) across 21 USG executive branch organizations.

After identifying the information assets, we coded them according to the key topic(s) they addressed. In many cases (e.g.: wmd; access to information, cyber security) we found multiple organizations (or multiple offices within a single organization) with assets related to a specific topic.[9] Across the entire initial list of information assets we identified and coded 1,305 unique information topics and classified these according to 13 categories: DIMEFIL (diplomatic, information, military, economic, finance, intelligence, and law enforcement); *plus* governance, social, national and cyber security, the physical environment and infrastructure. To increase the US-DiGIA's utility to SOCOM analysts and planners concerned with gray zone activities, the subset of information topics relevant to gray zone challenges was coded according to a separate, tailored gray zone coding scheme[10]. Figure I below provides an overview of our search and coding procedure.

[6] A full discussion of the coding rules used for constructing the US-DiGIA Directory is provided in the methodology report, available on the SMA publications website: http://nsiteam.com/sma-publications/.

[7] This variation in depth of information provided on a website can partly be explained by the nature of the work done. For example, the CIA website is sparse on detail, whereas outward-facing agencies such as USAID provide detailed reports and fact sheets on their work.

[8] We included all 12 executive departments in our initial information search, however we found no information assets relevant to national security or foreign policy in the Department of Housing and Urban Development and thus dropped that department from the final directory.

[9] Almost all federal departments and independent agencies possess sub-ordinate units to carry out discrete functions of the Department or Agency. In the US-DiGIA directory, all sub-ordinate units are referred to as "offices," irrespective of how the organization refers to it. In using this common term, our data organization posits that what is most important for this information mapping is not at what level of the hierarchy the sub-ordinate unit is located, but rather, which specified domains of expertise that unit possesses.

[10] See Part 2 of this report for a more detailed discussion of the gray zone coding scheme.

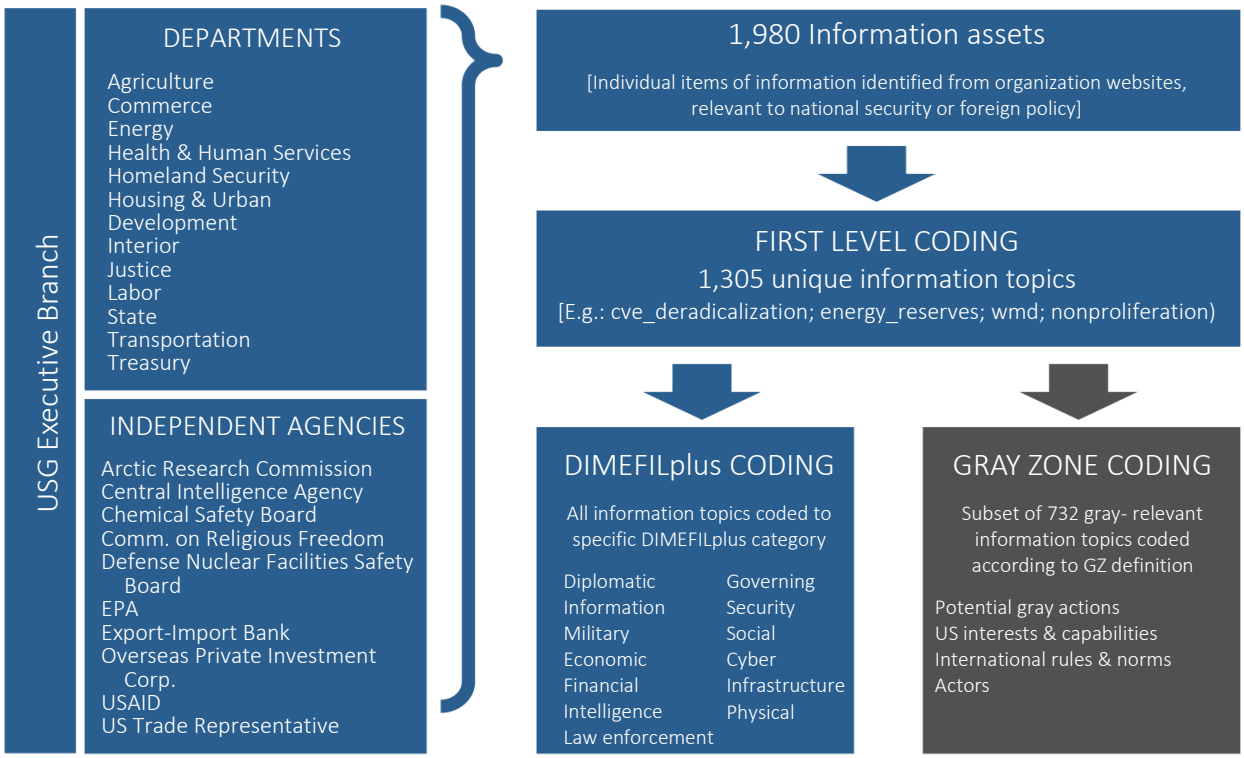



Figure 17: Information Search and Coding Procedure for US-DiGIA

Care should also be taken in interpreting the geographic area that the information assets cover—the "where." There was considerable variation in the specificity of the reported geographic scope of information assets. A further challenge is that there does not appear to be a standard set of geographic regions employed by USG organizations. As a result of these variations in the precision with which we could identify the geographic focus of information assets, we consider geography at two levels: 1) a US/ international dichotomy; and 2) where possible, a more specific coding by country or region.