### DSS Counterintelligence

#### Methods of Operation & Methods of Contact Matrix

<table>
<thead>
<tr>
<th>Method of Contact</th>
<th>Conference, Conventions or Trade Shows</th>
<th>Cyber Operations</th>
<th>Email Request</th>
<th>Foreign Visit</th>
<th>Personal Contact</th>
<th>Phishing Operations</th>
<th>Resume - Academic</th>
<th>Resume - Professional</th>
<th>Social or Professional Networking</th>
<th>Telephone</th>
<th>Web Form Submission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attempted Acquisition of Technology</td>
<td>L</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>M</td>
</tr>
<tr>
<td>Exploitation of Commercial/Business Activities</td>
<td>M</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>L</td>
</tr>
<tr>
<td>Exploitation of Cyber Operations</td>
<td>H</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>L</td>
</tr>
<tr>
<td>Exploitation of Experts</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>M</td>
</tr>
<tr>
<td>Exploitation of Insider Access</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>L</td>
</tr>
<tr>
<td>Exploitation of Relationships</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>L</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>M</td>
</tr>
<tr>
<td>Exploitation of Security Protocols</td>
<td>M</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td></td>
<td></td>
<td></td>
<td>L</td>
</tr>
<tr>
<td>Exploitation of Supply Chain</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>L</td>
</tr>
<tr>
<td>Resume Submission</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>L</td>
<td></td>
<td></td>
<td></td>
<td>L</td>
</tr>
<tr>
<td>RFI/Solicitation</td>
<td>H</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Search/Seizure</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Surveillance</td>
<td>M</td>
<td>L</td>
<td>L</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>L</td>
</tr>
<tr>
<td>Theft</td>
<td>M</td>
<td>L</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>M</td>
</tr>
</tbody>
</table>
Methods of Contact

- **Conference, Conventions, or Tradeshows**: Contact regarding or initiated during an event, such as a conference, convention, exhibitions, or tradeshow.
- **Email**: Unsolicited requests received via email for information or purchase requests.
- **Mail**: Contact initiated via mail or post.
- **Phishing Operation**: Emails with embedded malicious content or attachments for the purpose of compromising a network to include but not limited to spear phishing, cloning, and whaling.
- **Résumé - Academic**: Resume or CV submissions for academic purposes.
- **Social Networking Service**: Contact initiated via a social or professional networking platform.
- **Telephone**: Contact initiated via a phone call by a professional networking platform.

Methods of Operation

- **Cyber Operations**: Activities taken directly against a targeted system; to include cyber network attack, cyber network exploitation, and collection.
- **Foreign Visit**: Activities or contact occurring before, during, or after a visit to a contractor’s facility.
- **Personal Contact**: Person-to-person contact via any means where the foreign actor, agent, or co-optee is in direct or indirect contact with the target.
- **Résumé - Professional**: Resume or CV submissions for professional purposes. (e.g., seeking a position with a cleared company).
- **Web Form**: Contact initiated via a company-hosted web submission form.

Exploitation of Technology

- **Acquiring protected information in the form of controlled technologies, via direct contact or through the use of front companies or intermediaries, including the equipment itself or diagrams, schematics, plans, spec sheets, or the like.**

Exploitation of Cyber Operations

- **Foreign intelligence entities or other adversaries exploiting the confidentiality, integrity, or availability of targeted networks, applications, credentials or data with the intent to gain access to, manipulate, or exfiltrate personnel information or protected information and technology.**

Exploitation of Insider Access

- **Trusted insiders exploiting their authorized placement and access within cleared industry or cause other harm to compromise personnel or protected information and technology.**

Exploitation of Security Protocols

- **Visitors or unauthorized individuals circumventing or disregarding security procedures or behaviors by cleared or otherwise authorized persons that indicate a risk to personnel or protected information and technology.**

Exploitation of Business Activities

- **Establishing a commercial relationship via joint ventures, partnerships, mergers and acquisitions, foreign military sales, or service provider; leveraging an existing commercial relationship in order to obtain access to personnel or protected information and technology.**

Exploitation of Experts

- **Gaining access to personnel or protected information and technology via requests for, or arrangement of, peer or scientific board reviews of academic papers or presentations; requesting a consult with faculty members or subject matter experts; or attempting to invite or otherwise entice subject matter experts to travel abroad or consult for foreign entities.**

Exploitation of Relationships

- **Leveraging existing personal or authorized relationships to gain access to protected information.**

Exploitation of Supply Chain

- **Compromising the supply chain, which may include the introduction of counterfeit or malicious products or materials into the supply chain with the intent to gain unauthorized access to protected data, alter data, disrupt operations, or interrupt communication.**

RFI/Solicitation

- **Collecting protected information by directly or indirectly asking or eliciting personnel or protected information and technology.**

Surveillance

- **Systematically observing equipment, facilities, sites, or personnel associated with contracts via visual, aural, electronic, photographic, or other means to identify vulnerabilities or collect information.**

Created by the Defense Security Service Counterintelligence Directorate
Contact us at dss.quantico.dss-hq.mbx.ci-production@mail.mil

Distinct patterns or methods of procedure thought to be characteristic of or habitually followed by an individual or organization involved in intelligence activity. These generally include attempts at: