Geheime Post. Kryptologie und Steganographie der diplomatischen Korrespondenz europäischer Höfe während der Frühen Neuzeit

Veranstalter: Forschungsbibliothek Gotha, Schloss Friedenstein
Datum, Ort: 14.02.2013–16.02.2013, Gotha
Bericht von: André Bochynski, Gotha

Wissenschaftler aus verschiedenen Bereichen der Diplomatie-, Wissenschafts- und Kulturgeschichte trafen in den historischen Räumen von Schloss Friedenstein in Gotha auf einer internationalen Tagung zusammen, um in insgesamt sieben Sektionen über aktuelle Forschungen zur Verschlüsselung sowie verborgenen Korrespondenzen zu diskutieren. Eingeladen hatte das Forschungszentrum Gotha der Universität Erfurt in Kooperation mit der Kollegforschergruppe „Religiöse Individualisierung in historischer Perspektive".

Bei der Übermittlung von brisanten Informationen in der Zeit zwischen 1500 und 1815 wurden sowohl verborgene (steganographische) als auch verschlüsselte (kryptographische) Informationsweiterleitung genutzt. Diese Praxis der Geheimhaltung lässt sich dabei anhand chiffrierter Briefe sowie überlieferter Kanzleiakten nachvollziehen. Eine Erforschung dieser Phänomene der Diplomatiegeschichte beschränkt sich in der gegenwärtigen Forschungslandschaft jedoch eher auf den Bereich von Überblicksdarstellungen zu den Methoden des Verschlüsselns unter besonderer Konzentration auf das 20. Jahrhundert. Die Tagungsleitung stellte es sich daher zur Aufgabe, einen transdisziplinären Fokus auf die Erforschung der Gesandtschaftsgeschichte zu richten und die Praktiken der Geheimhaltung von Korrespondenzen in Hinblick auf die konkreten Entschlüsselungsmethoden, die Taktiken des Einsatzes sowie die Chiffrierungssysteme zu betrachten. Die Diskussion wandte sich speziell der räumlichzeitlichen Ebene sowie der personellen und der praktischen Perspektive einer Geheimkorrespondenz europäischer Höfe zu. Neben renommierten Experten zur Geschichte der Geheimdiplomatie waren auch zahlreiche Nachwuchsforscher anwesend.

Eröffnet wurde die Tagung durch ANNE-SIMONE ROUS (Gotha), die von ihrer Habilitationsschrift zur Geheimdiplomatie in der Neuzeit berichtete und über „Perspektivenwechsel zum Phänomen der Informationssicherheit in der diplomatischen Korrespondenz der Frühen Neuzeit" vortrug. Sie ging hierbei auf die Bedeutung eines Wissensvorsprungs gegenüber einem Gegner ein, welche sich durch einen Vorrang in der Nachrichtenübermittlung ergibt. Das sich hieraus ergebende fortdauernde Streben nach Absicherung der eigenen Kommunikationswege sowie gleichzeitiger Enttarnung feindlicher Verständigung bildete den Motor eines sich ausdifferenzierenden Systems der Verschlüsselung und Dekodierung. Der Beitrag formulierte Thesen zu möglichen Zielen und Taktiken des neuzeitlichen Informationswettlaufs.

Anschließend beschäftigte sich KARL DE LEEUW (Amsterdam) in seinem Beitrag mit möglichen Methoden geheimer Kommunikation. Hierbei erörterte er den Einfluss neuerer Schwarzer Kabinette in Russland sowie den Niederlanden auf die sichtbare Verbreitung des zuvor geheim gehaltenen kryptoanalytischen Wissens als Folge des Zusammentreffens unterschiedlicher Spionageformen sowie der Zunahme des wissenschaftlichen Denkens während des 18. Jahrhunderts. Zudem arbeitete er auch einen Zusammenhang von Kryptologie und wissenschaftlicher Spezialisierung durch die Entfaltung empirischer Methoden heraus. De Leeuw ging unter anderem auf den Mathematiker und Physiker Willem Jacob's Gravesande ein, der sich neben der praktischen Vermittlung von Naturgesetzen auch als Entzifferer im Spanischen Erbfolgekrieg verdient machte. In diesem Sinne war er der Erste, der anhand von Häufigkeitsstatistiken die Methode zur Entschlüsselung ableitete und diese durch sorgfältige Thesenformulierung und Operationalisierung an die unerwarteten Resultate anpasste.

Im Anschluss daran machte KLAUS SCHMEH (Gelsenkirchen) auf aktuelle Desiderate der Forschung aufmerksam. Da es an Analysematerial mangele sei eine Zusammenführung verschiedener Forschungszweige in einer gemeinsamen Plattform eine Möglichkeit, Ressourcen zu bündeln und Forschungsfragen interdisziplinär zu klären. Die sich aus dem Quellenmaterial selbst

ergebenden Fehlerquellen, wie etwa eine erschwerte Transliteration, Schreibfehler oder Unkenntnis der Dechiffrierung unverständlicher Sprachen, könnten auf diesem Wege im Verbund diskutiert werden. Gerade die Bestände neuzeitlicher Geheimschriften böten im Vergleich zur modernen Kryptoanalyse aufgrund anderer interdisziplinärer Verfahren (Linguistik, Technik, Statistik) völlig neue Gelegenheiten, sich den Methoden und Hintergründen historischer Verschlüsselungen zu widmen und eine umfassende Theorie zu frühmodernen Verschlüsselungspraktiken zu formulieren.

Das Beispiel einer interdisziplinären Entschlüsselungsleistung zeigte CHRISTIANE SCHAEFER (Uppsala) in ihrem Beitrag. Im Verbund mit einem Forscherteam aus Schweden und den USA gelang es ihr 2011 ein Manuskript aus der zweiten Hälfte des 18. Jahrhundert vollständig zu entschlüsseln und somit historisch einzuordnen. Durch computergestützte Methoden sowie vergleichenden linguistischen Frequenzstatistiken konnte so ein „Gesetz der Okulistengesellschaft" in Klartext zurückgeführt werden, was zu einer beachtlichen Neuinterpretation der Zielsetzungen der Gesellschaft selbst führte. In der Folge entstand der Plan, die interaktive digitale Datenbank *CADMUS* zu entwickeln, die dem Nutzer verschiedene Chiffrentypen der Frühen Neuzeit auch in Form quantitativ großer Textgrundlagen bietet und dadurch computerlinguistischen Methoden der Forschung zur Verfügung stellt.

Die Diskussion evidenter Forschungsprobleme wurde durch MICHAEL KOREY (Dresden) weitergeführt, der am Beispiel zweier sächsischer Verschlüsselungsgeräte demonstrierte, wie sowohl die technischen Raffinessen als auch die Kunstfertigkeit bei der Hervorbringung von Chiffrierungswerkzeugen die Aufmerksamkeit eines Landesherren auf sich ziehen konnten. Hierbei wies Korey anhand typischer Sammlungsobjekte des kursächsischen Hofes darauf hin, dass entgegen der zeitgenössischen Meinung auch in deutschen Territorien die Fähigkeit zur Verschlüsselung durchaus meisterlich betrieben wurde.

Den Abendvortrag gestaltete GERHARD STRASSER (Pennsylvania/Landshut) zum Thema „Die Wissenschaft der Alphabete. Universalsprachen vom 16. bis zum frühen 19. Jahrhundert im Kontext von Kryptographie und Philosophie". Er vereinte die Themenkomplexe von Kryptologie und Germanistik ausgehend von den Chiffren des Abtes Johannes Trithemius, die in späteren Jahrhunderten als Inspiration etwa bei Athanasius Kircher zur Entwicklung einer Universalsprache im Sinne einer algorithmischen Linguistik dienten. Auf dieser Grundlage habe auch Gottfried Wilhelm Leibnitz Versuche unternommen, eine philosophische *lingua franca* zu entwickeln. Darüber hinaus machte Strasser auf die Versuche Herzog Augusts II. von Braunschweig [U+2010] Wolfenbüttel aufmerksam, der unter dem Pseudonym Gustavus Selenus selbst Schriften zur Kryptographie verfasste und zudem auch mit Kircher eine Korrespondenz unterhielt.

Zur Veranschaulichung kryptographischer Systeme präsentierte FILIPPO SINAGRA (Mestre) Beispiele frühneuzeitlicher Originalquellen der italienischen Geheimhaltungspraxis. Er erläuterte Chiffrensysteme, Nomenklaturen und Entschlüsselungswerkzeuge, die in verschiedensten kryptographischen Dienste der Sforza aktive Verwendung fanden.

Ein interessantes Gegenbeispiel zum dienlichen Einsatz von Verschlüsselungstaktiken zur Weiterleitung von Nachrichten präsentierte MARTIN SKOERIES (Leipzig). Ausgehend von den Rekatholisierungsmaßnahmen seit 1553 unter Maria I. Tudor waren viele einflussreiche Theologen dazu gezwungen, angesichts der drohenden Lebensgefahr ein clandestines Kommunikationsnetzwerk aufzubauen. Das Schmuggeln von Nachrichten oder die mehrfache Kopie von Briefen sollte zudem die Wahrscheinlichkeit erhöhen, zumindest einige wenige Zeugnisse aus den Gefängnissen in die Öffentlichkeit zu bringen und die katholische Herrschaft propagandistisch zu untergraben. In der Auswertung nikodemitischer Gefangenenkorrespondenzen hinsichtlich der sozialen Beziehungen der Autoren untereinander konnte festgestellt werden, dass auf eine Verschlüsselung von Seiten der Verfolgten bewusste verzichtet wurde, damit abgefangene Korrespondenzen als Beweis für das erlittene Martyrium dienen konnten.

Ein eigenes Themengebiet im Umgang mit Chiffrierungsmethoden bildete das Haus Habsburg. Hierzu erörterte CAROLIN PECHO (Paderborn) die verschiedenen Anwendungsmomente der Textverschlüsselung in der Privatkorrespondenz des Erzherzogs Ferdinands von Österreich (später Kaiser Ferdinand II.) mit seinem Bruder Leopold während der Auseinandersetzungen um Jülich und Kleve 1609. Diese hätten wiederkehrend auf Textverschlüsselungen zurückgegriffen, wobei sich vom heutigen Standpunkt aus weniger ein codieren brisanter Informationen erkennen lasse, als vielmehr eine in der gemeinsamen Kindheit erlernte Kommunikationsweise. Diese kann als ein bewusst eingesetztes Stilmittel der brüderlichen Zuneigung in Zeiten familiärer Konkurrenz und gegenseitige Vergewisserung verstanden werden.

In diesem Zusammenhang betrachtete auch LEOPOLD AUER (Wien) „Die Verwendung von Chiffren in der diplomatischen Korrespondenz des Kaiserhofes im 17. und 18. Jahrhundert“. Hierbei machte er auf die Zuständigkeit und Zusammenarbeit von geheimen Abteilungen der Kanzleien auf die Chiffrendepartements der habsburgischen Reichs[U+2010] und Hofkanzleien sowie der späteren Geheimen Kabinettskanzlei aufmerksam. In diesem Zusammenhang wies Auer auf die Überlieferungssituation hin, die sich neben den erhaltenen Chiffrenschlüsseln, ver[U+2010] und entschlüsselten Texten sowie wenigen Personalunterlagen beteiligter Personen zusammensetzt. Aus den Methoden und dem Aufwand der Entschlüsselung muss dabei der institutionelle Rahmen rekonstruiert werden, der auch die Archivierung unaufgelöster Texte sowie verwendeter Nomenklaturen bestimmte und die diplomatische Korrespondenz des Kaiserhofes in der Qualität der Verschlüsselungsmethode variieren ließ.

Einen Abschluss fand diese Sektion durch den Vortrag über „Die chiffrierte Post Wien-Istanbul um 1700“ von GERHARD KAY BIRKNER (Hamburg). Ausgehend vom protokollarischen Verlauf der Gesandtschaftsreise des Reichshofratspräsidenten Wolfgang IV. von Oettingen[U+2010]Wallerstein an den Osmanischen Hof 1699 bildeten die geheim gehaltenen Verhandlungen über Patronatsrechte und Grenzverläufe zwischen dem Wiener Hof und der Gesandtschaft einen zentralen Teil der weiteren diplomatischen Verhandlungen. Die für diesen Zweck speziell entwickelte Chiffriertabelle ist hierbei ebenso wie das Dechiffrierbuch Wallersteins erhalten und demonstriert die ungebrochene Anwendung der Kryptographie in Gegenwart politisch labiler Situationen. Birkner erörterte in der Folge die Beibehaltung und Weiterentwicklung der Kodierung einzelner Buchstaben und Silben hin zu differenzierten Nomenklaturen relevanter Begriffe.

Den Habsburgern gegenüber wurde folgend auch das Haus Wettin und dessen Chiffrierungstaktiken vor allem unter dem sächsisch-polnischen Herrscher August II. in den Blick genommen. MARIUSZ WIESŁAW KACZKA (Gießen) wandte sich der Korrespondenz zwischen den rumänischen Fürsten von Moldau und der Walachei zu. Da diese von Osmanischer Seite verboten war, bedienten sich die rumänischen Fürsten unterschiedlichster Verschlüsselungsmethoden, um mit anderen Donaufürstentümern sowie christlichen Staaten in Kontakt zu treten. Anhand des Beispiels des umfangreichen Schriftwechsels des walachischen Fürsten Constantin Brâncoveanu mit August dem Starken thematisierte Kaczka die hierbei aufgetretenen Geheimhaltungsmethoden. Zudem zeichnete er anhand zeitgenössischer Karten die Kommunikationswege zwischen Warschau, Dresden, Bukarest und Istanbul nach.

Weiterführend beschäftigte sich HOLGER KÜRBIS (Frankfurt am Main) mit der Gesandtschaft des kursächsischen Legationssekretärs Johann Bendikt Wolters am Gothaer Hof im Jahre 1702. Hierbei ging er auf den Gothaer Herzog Friedrich II. und dessen Kontakte zu August II. von Sachsen ein. Dieser unterrichtete seinen albertinischen Vetter über das Vorgehen dänischer Truppen unter anderem in den eigenen Landen und bat ihn um Unterstützung. In der Folge entsandte der kursächsische Hof einen Sekretär samt Instruktionen zur Korrespondenzverschlüsselung nach Gotha. Der Code, der nur in den persönlichen Depeschen an den Monarchen angewandt wurde, bestand hierbei aus einer dreifach monoalphabetischen Verschlüs-

selung. Die Betonung der Vorzüge der Chiffre durch den Legationssekretär trotz der seltenen Anwendung unterstreicht abermals die empfundene Bedeutsamkeit seiner Unternehmung und eine theoretische Notwendigkeit der Verschlüsselung.

Dieser Sektion wurde das Beispiel Frankreich gegenübergestellt. In diesem Sinne ging JÖRG ULBERT (Lorient) den „Sicherungsmaßnahmen in französischen Diplomaten und Konsularkorrespondenzen (1650–1730)" nach. Ausgehend von den Friedenskongressen seit der Mitte des 17. sowie des beginnenden 18. Jahrhunderts, kann ein sich beschleunigender Modernisierungsprozess innerhalb der europäischen Diplomatie ausgemacht werden. Hierbei falle zudem eine Spezialisierung der Postspionage auf. Daraus entwickelten sich, nach Ulbert, unter anderem in der französische Zentralverwaltung verschiedenste Gegenmaßnahmen innerhalb des Konsular- sowie des Diplomatiewesens zur Absicherung des Briefverkehrs. Zu nennen wären etwa die Einrichtung von Deckadressen, die Überwachung der Zustellwege und -zeiten sowie die Verschlüsselung des Inhalts selbst. Der Beitrag stellte verschiedenste Sicherungsmethoden aus den Beständen des Archives des Affaires étrangères Paris vor und erörterte diese in Hinblick auf ihre Effizienz.

In diesem Zusammenhang besprach auch ANDREAS AFFOLTER (Bern) „Geheimhaltungspraktiken in den Korrespondenzen des französischen Ambassadors in der Eidgenossenschaft im frühen 18. Jahrhundert. Vor dem Hintergrund des komplexen Bündnissystems der Eidgenossenschaft seien fremde Gesandtschaften dazu gezwungen gewesen, aufgrund eines fehlenden Machtzentrums ein Netzwerk von Vertrauensleuten zu unterhalten, welche sie mit den erforderlichen Berichten versorgten. Die Korrespondenz des Marquis d'Avaray stelle in diesem Sinne eine der wenigen überlieferten Quellensammlung dar, welche einen Einblick in die Verschlüsselungsmethoden der eidgenössischen Magistrate gegenüber französischen Gesandten zulasse. Abermals wurde hier die Frage danach aufgeworfen, welche Informationen überhaupt als verschlüsselungswürdig angesehen wurden und wann bewusst auf eine Chiffrierung verzichtet wurde.

Die letzte Sektion zum Ausgang der Frühen Neuzeit eröffnete BENJAMIN BÜHRING (Göttingen) mit Ausführungen über Postspionage in der Personalunion Großbritannien-Hannover. Hierbei ging er auf die diplomatische Korrespondenz zwischen der Deutschen Kanzlei in London sowie den Geheimen Räten in Hannover unter Georg I. und Georg II. ein und erörterte – ausgehend von den unterschiedlichen Abstufungen von Vertrauensbildung – die Entwicklung und Spezialisierung der Postspionage sowie Versuche, gegnerische Bespitzelungen zu unterlaufen. Dabei sei das Abfangen von Post, das Siegelfälschen, das Kopieren von Briefe bzw. die Entschlüsselung des verborgenen Inhalts mit der Entwicklung des Sicherungssystems der Post sowie der Ausbildung des dazugehörigen Personals einhergegangen.

Ebenso setzte sich ANDREAS ÖNNERFORS (Malmö) mit einer diplomatischen Mission nach Großbritannien auseinander. Am Beispiel des schwedische Barons Jöran Ulrik Silfverhielm, der 1797 neben der Repräsentation machtpolitischer Interessen Schwedens auch vertrauliche Verbindungen zur Freimaurerei unterhielt, besprach Önnerfors die geheim gehaltene Korrespondenz des Diplomaten mit seinen Auftraggebern in Stockholm. Die Korrespondenz Silfverhielms, die in Zusammenhang mit dem „Unlawful Societies Act" (1799) – einem Verbot der Freimaurerei aufgrund der sich verhärtenden innenpolitische Konspirationsdiskurses steht – erlaube in diesem Zusammenhang einen Einblick in die Überschneidungen sowohl politischer als auch clandestiner Diplomatie.

Abschließend führte OLIVER BENJAMIN HEMMERLE (Grenoble) in die vor allem vor dem militärischen Hintergrund genutzten Verschlüsselungssysteme unter Napoléon Bonaparte ein. Dabei thematisierte er Probleme der Codierung der kaiserlichen Korrespondenz und machte einmal mehr darauf aufmerksam, dass das fehlende Wissen hinsichtlich frühneuzeitlicher Chiffrierungsmethoden aufgrund fehlender Schlüssel den aktuellen Kenntnismangel begründe, was auch die entsprechende Historiographie und Klischeebildung seit dem 19. Jahrhunderts geprägt habe.

Zusammenfassend kann festgestellt wer-

den, dass die Tagung sowohl durch die fach- als auch epochenübergreifenden Leistungen einen neuralgischen Punkt der diplomatiegeschichtlichen Aufforschung freigelegt hat. Das Konzept von geographisch übergreifenden und sich ergänzenden Vergleichsstudien führte zu einer reichen Diskussion über den Umgang mit der Notwendigkeit militärisch-politischer Geheimhaltung einerseits sowie den nachweisbaren Handlungsweisen der Nachrichtenverschlüsselung und Postspionage auf der anderen Seite. Ein wichtiges Ergebnis zeigt sich in der Beschaffenheit der chiffrierten Nachrichten selbst, welche aus heutiger Betrachtung oftmals keine geheimzuhaltenden Informationen zu enthalten scheinen. Im Gegensatz dazu wurde das wiederkehrende Phänomen bestätigt, dass offensichtlich brisante Auskünfte häufig als Klartext abgefasst wurden. Neben einer erwünschten Erforschung von Verschlüsselungstaktiken in Friedenszeiten stellt vor allem der Umgang mit den personellen Trägern des diplomatischen Schriftverkehrs ein sich für zukünftige Forschungen ergebender Schwerpunkt dar. Es sind die Geheimsekretäre selbst als auch ihre Auftraggeber, die Netzwerke ihrer Agenten sowie die Kreise der Kryptologen und Chiffrensekretäre zur Konstruktion und Erarbeitung der immer noch komplexen Verschlüsselungssysteme, die eine bis jetzt nur ungenügend untersuchte Personengruppe bilden.

Konferenzübersicht

Anne-Simone Rous (Gotha): Geheime Post und Interzeption – Perspektivenwechsel zum Phänomen der Informationssicherheit in der diplomatischen Korrespondenz der Frühen Neuzeit

Karl de Leeuw (Amsterdam): Thesen und Forschungsfragen zur Geschichte der frühmodernen Kryptologie

Klaus Schmeh (Gelsenkirchen): Dechiffrierung verschlüsselter Texte der frühen Neuzeit – Methoden, Probleme, Forschungsbedarf

Christiane Schaefer (Uppsala): Der Codex Copiale – ein Forschungsbericht über die Geheimschrift der Oculisten und Ausgangspunkt für ein Kryptographie[U+2010]Projekt der Computerlinguistik

Michael Korey (Dresden): Versteckte Steganographie und verbrannte Substitution. Einige wenig bekannte Chiffriergeräte aus der Dresdner Kunstkammer

Gerhard Strasser (Pennsylvania/Landshut): Die Wissenschaft der Alphabete. Universalsprachen vom 16. bis zum frühen 19. Jahrhundert im Kontext von Kryptographie und Philosophie

Filippo Sinagra (Mestre): La diplomazia Sforzesca und die Kryptographie in Italien im 16. Jahrhundert (1450–1600)

Martin Skoeries (Leipzig): ‚It is death for any to speak with me'. Über die Kommunikation verfolgter englischer Protestanten unter ‚Bloody Mary' (1553–1558)

Carolin Pecho (Paderborn): „Der Habsburger-Code. Chiffrierte Briefe von Erzherzog Ferdinand an Erzherzog Leopold während des Erbfolgekrieges um Jülich-Kleve (1609–1610)

Leopold Auer (Wien): Die Verwendung von Chiffren in der diplomatischen Korrespondenz des Kaiserhofes im 17. und 18. Jahrhundert

Gerhard Kay Birkner (Hamburg): Die chiffrierte Post Wien-Istanbul um 1700

Mariusz Wiesław Kaczka (Gießen): Geheimdiplomatie und Spionage zwischen Warschau, Dresden, Bukarest, Iași und Istanbul im ausgehenden 17. Jahrhundert

Holger Kürbis (Frankfurt am Main): Gesandtschaft des kursächsischen Legationssekretärs Johann Bendikt Wolters am Gothaer Hof im Jahre 1702

Jörg Ulbert (Lorient): Sicherungsmaßnahmen in französischen Diplomaten und Konsularkorrespondenzen (1650–1730)

Andreas Affolter (Bern): Geheimhaltungspraktiken in den Korrespondenzen des französischen Ambassadors in der Eidgenossenschaft Claude-Théophile de Bésiade, Marquis d'Avaray, (1716–1726)

Benjamin Bühring (Göttingen): Vertrauensbildende Maßnahmen – Die Bedeutung des Postwesens, Postspionage und die Sicherung

von Korrespondenz am Beispiel der dynastischen Union zwischen Kurhannover und Großbritannien

Andreas Önnerfors (Malmö): Schwedische diplomatische Korrespondenz über die britische ‚Unlawful Societies Act' (1799)

Oliver Benjamin Hemmerle (Grenoble): Napoleon entziffern: Historiographie und Probleme der Kryptologie zu Zeiten des ‚1er Empire'

Tagungsbericht *Geheime Post. Kryptologie und Steganographie der diplomatischen Korrespondenz europäischer Höfe während der Frühen Neuzeit*. 14.02.2013–16.02.2013, Gotha, in: H-Soz-Kult 19.06.2013.